460MSBS - Protocol Gateway

Product User Guide

Software Build Date: January 15th, 2015
Revision 3

Trademarks

CompactLogix, ControlLogix, & PLC-5 are registered trademarks of Rockwell Automation, Inc. EtherNet/IP is a trademark of the ODVA. MicroLogix, RSLogix 500, and SLC are trademarks of Rockwell Automation, Inc. Microsoft, Windows, and Internet Explorer are registered trademarks of Microsoft Corporation. BACnet® is a registered trademark of American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE). All other trademarks and registered trademarks are the property of their holders.

Limited Warranty

Real Time Automation, Inc. warrants that this product is free from defects and functions properly.

EXCEPT AS SPECIFICALLY SET FORTH ABOVE, REAL TIME AUTOMATION, INC. DISCLAIMS ALL OTHER WARRANTIES, BOTH EXPRESSED AND IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR APPLICATION. THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY ALSO HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE.

The examples and diagrams in this manual are included solely for illustrative purposes. Because of the many variables and requirements associated with any particular application, Real Time Automation, Inc. cannot assume responsibility or liability for actual use based on the examples and diagrams. Except as specifically set forth above, Real Time Automation and its distributors and dealers will in no event be liable for any damages whatsoever, either direct or indirect, including but not limited to loss of business profits, income, or use of data. Some states do not allow exclusion or limitation of incidental or consequential damages; therefore, the limitations set forth in this agreement may not apply to you.

No patent liability is assumed by Real Time Automation with respect to use of information, circuits, equipment, or software described in this manual.

Government End-Users

If this software is acquired by or on behalf of a unit or agency of the United States Government, this provision applies: The software (a) was developed at private expense, is existing computer software, and was not developed with government funds; (b) is a trade secret of Real Time Automation, Inc. for all purposes of the Freedom of Information Act; (c) is “restricted computer software” submitted with restricted rights in accordance with subparagraphs (a) through (d) of the Commercial “Computer Software-Restricted Rights” clause at 52.227-19 and its successors; (d) in all respects is proprietary data belonging solely to Real Time Automation, Inc.; (e) is unpublished and all rights are reserved under copyright laws of the United States. For units of the Department of Defense (DoD), this software is licensed only with “Restricted Rights”: as that term is defined in the DoD Supplement of the Federal Acquisition Regulation 52.227-7013 (c) (1) (ii), rights in Technical Data and Computer Software and its successors, and: Use, duplication, or disclosures is subject to restrictions as set forth in subdivision (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at 52.227-7013. If this software was acquired under GSA schedule, the U.S. Government has agreed to refrain from changing or removing any insignia or lettering from the Software or documentation that is provided or from producing copies of the manual or media. Real Time Automation, Inc.

© 2015 Real Time Automation, Inc. All rights reserved.

Overview 5
Required Tools and Data 6
Powering The Gateway 7
Accessing the Main Page 8
Error: Main Page Does Not Launch 9
Main Page 10
Device Configuration 11
Modbus TCP/IP Server Configuration 12
Modbus TCP/IP Server Configuration-Data Groups 13
Modbus TCP/IP Server Data Group Configuration: Auto-Server Mode (Default) 14
Modbus TCP/IP Server Data Group Configuration: Manual Mode 15
BACnet/IP Server Configuration 17
BACnet/IP Server Configuration-Data Groups 18
BACnet/IP Server Configuration: Auto-Server Mode (Default) 19
BACnet/IP Server Configuration: Manual Mode 19
BACnet/IP Server Object Configuration – Analog Objects 20
BACnet/IP Server Object Configuration – Binary Objects 21
BACnet/IP Server Object Configuration – CharacterString Value Objects 22
BACnet/IP Server Object Configuration – Group Names 23
BACnet/IP Server Routing Configuration 24
Mapping - Transferring Data between Devices 25
Display Mapping and Values 26
Display Data 26
Display String 28
Data and String Mapping – Auto-Map 29
Data Mapping – Explanation 30
Data Mapping – Adding Diagnostic Information 31
String Mapping – Explanation 34
Mapping – Auto-Map Mode to Manual-Map Mode 35
Mapping – Manual-Map Mode to Auto-Map Mode 36
View Data Mapping as Text 37
View String Mapping as Text 38
Security Configuration 39
Security Configuration-Security Levels 40
Security - Log In 41

Security - Log Out 42
Email Configuration 43
Alarm Configuration 44
Diagnostics – Alarm Status 46
Alarms – Active 46
Alarms – Clear 47
Change of State (COS) Configuration 48
Diagnostics Info 49
Diagnostics – Data and String Mapping 49
Diagnostics – Modbus TCP/IP Server 50
Diagnostics – Modbus TCP/IP Server 51
Diagnostics – BACnet/IP Server 52
LED Configuration 55
Configuration Files 56
Export Configuration 56
Import Configuration 56
Utilities 57
Completing the Installation 58

Overview

The 460MSBS gateway connects a Modbus TCP Client device to a BACnet/IP Client. By following this guide, you will be able to configure the 460MSBS.

You will set the gateway's network settings, configure device specific parameters for initial operation, and integrate the device into your application.

For further customization and advanced use, please reference the appendices located on the CD. If at any time you need further assistance do not hesitate to call Real Time Automation support.

Support Hours are Monday-Friday 8am-5pm CST

Toll free: 800-249-1612
Email: support@rtaautomation.com

Required Tools and Data

You will need the following tools:

- The gateway
- The provided CD-ROM
    - IPSetup.exe can also be downloaded:

      http://www.rtaautomation.com/product/460-gateway-support/
- A PC with an internet browser
    - Browser configuration is Firefox / Internet Explorer / Google Chrome compatible
- The supplied Ethernet crossover cable
- A 7-30 VDC power source

Powering The Gateway

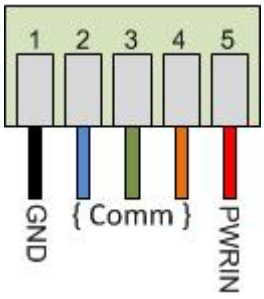
The following steps will allow you to properly and safely power the gateway.

Warning improper wiring will cause unit failure
Use the Barrel Connector OR the Screw Terminals power connection, NOT both

1. Connect a 24VDC power source to the gateway.

   a. The unit draws 125 mA at 24VDC

   b. The gateway has a voltage operating range from 8-30VDC, 24VDC is recommended.



Hazardous Environment Power & Installation Instructions

This equipment is suitable for use in Class I, Division 2, Groups A, B, C and D, or non-hazardous locations only.

WARNING – EXPLOSION HAZARD - Do not disconnect equipment unless power has been removed or the area is known to be non-hazardous.

WARNING – EXPLOSION HAZARD - Substitution of components may impair suitability for Class I, Division 2.

THIS EQUIPMENT IS OPEN-TYPE DEVICE AND IS MEANT TO BE INSTALLED IN AN ENCLOSURE SUITABLE FOR THE ENVIRONMENT SUCH THAT THE EQUIPMENT IS ONLY ACCESSIBLE WITH THE USE OF A TOOL.

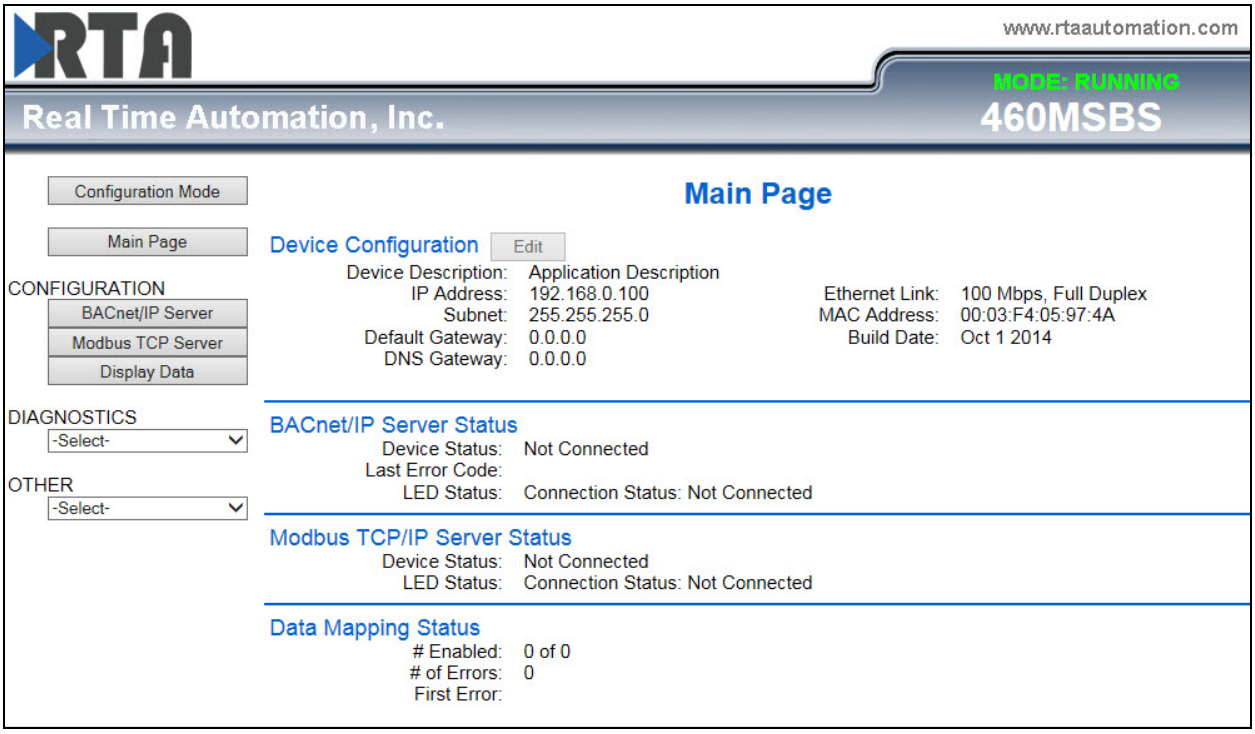
WARNING – POWER JACK (Barrel Connector, J1) IS FOR MAINTENANCE USE ONLY AND MAY ONLY BE USED WHILE THE AREA KNOWN TO BE FREE OF IGNITIBLE CONCENTRATIONS OF FLAMMABLE GASES OR VAPORS. IT IS NOT TO BE CONNECTED UNDER NORMAL OPERATION.

In Hazardous Environments the unit must be powered with between 12-24 VDC, 860 mA (6 W) max. Supervised. The unit is certified to be operated at -40°C to 50°C.

Accessing the Main Page

The following steps will allow you to connect to the browser based configuration of the gateway.

1. Using the supplied crossover cable, connect the gateway to your PC.
2. Insert the provided CD-ROM.
3. Run the IPSetup.exe program from the CD-ROM.
4. Configure the IP Settings of the gateway to be on the same subnet as your PC.
5. Click **Launch Webpage**. The Main page should appear.



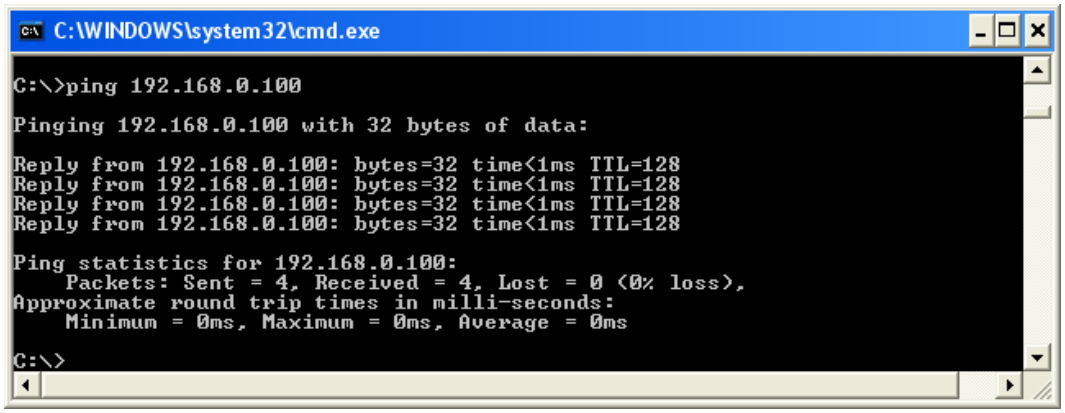
Default IP Address is 192.168.0.100.
Default Subnet is 255.255.255.0.

Error: Main Page Does Not Launch

If the Main Page does not launch please verify the following:

1. Check that the PC is set for a Static IP Address
    a. Open a MS-DOS Command Prompt
    b. Type “ipconfig” and press enter
    c. Note the PC’s IP Address, Subnet, and Default Gateway
        i. An invalid IP Address would be: 169.254.x.x
2. The gateway must be on the same Network/Subnet as the PC

Once you have both devices on the same network, you should be able to ping the gateway using a MS-DOS Command Prompt.



If you are able to successfully ping your gateway, open a browser and try to view the main page of the gateway by entering the IP Address of the gateway as the URL.

Main Page

The main page is where important information about your gateway and its connections are displayed.

Mode (orange box below):

Running Mode:

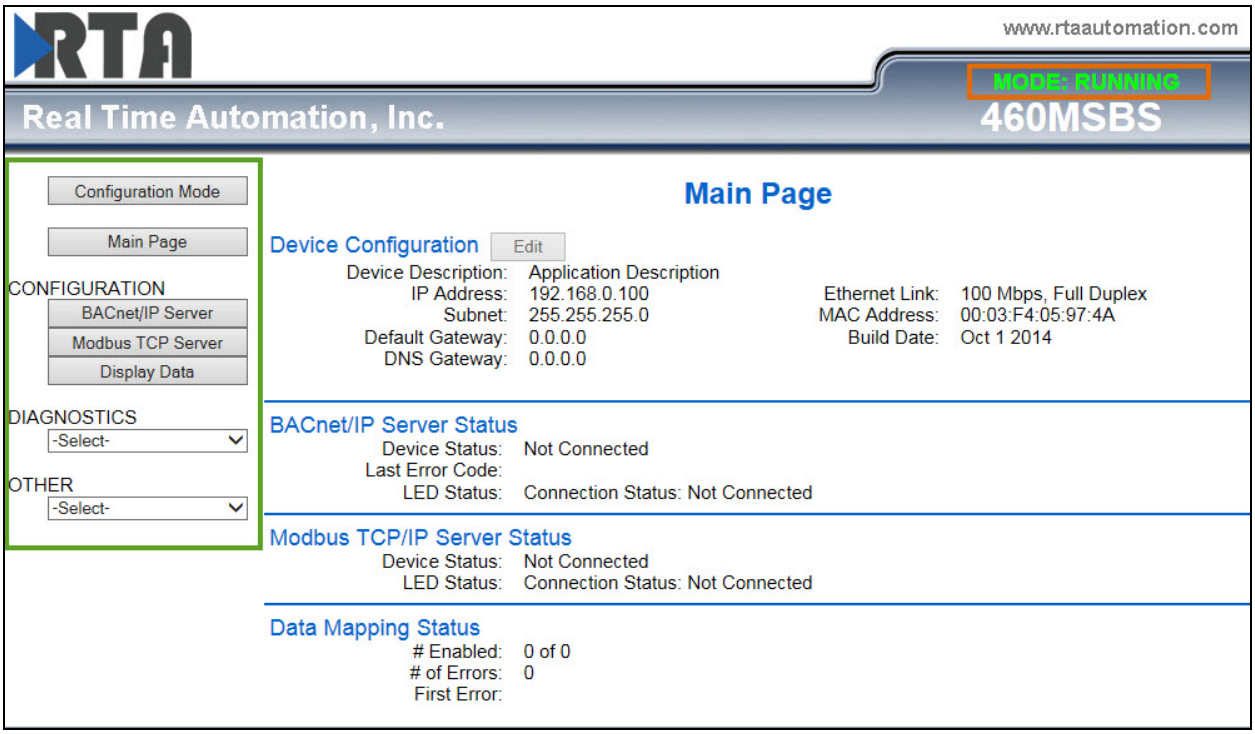
- Protocol communications are enabled
- Configuration cannot be changed during Running Mode. If changes are needed, click the **Configuration Mode** button shown in the green box below

Configuring Mode:

- Protocol communication is stopped and no data is transmitted
- Configuration is allowed

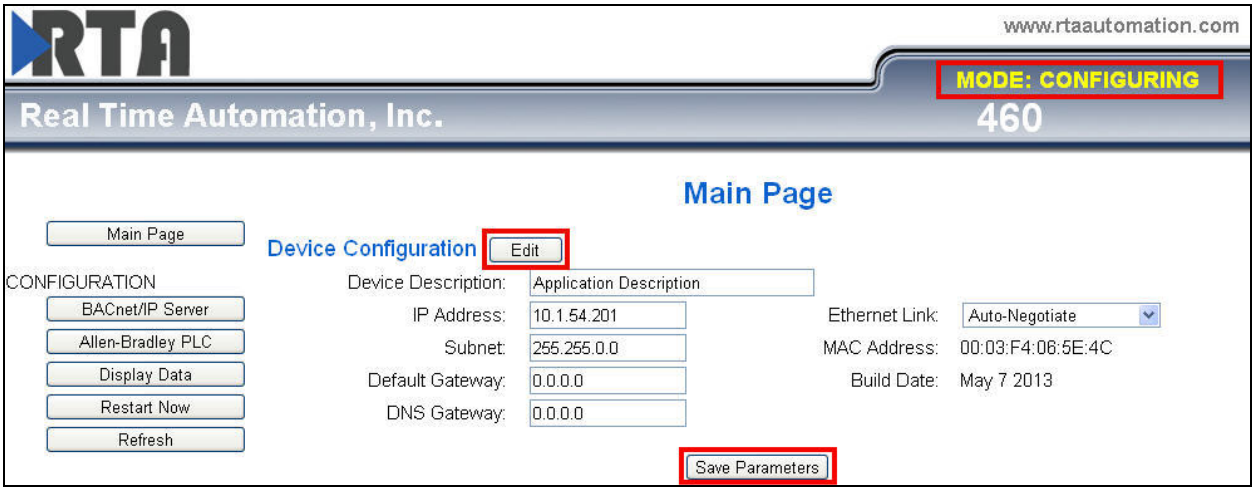
Navigation (green box below):

You can easily switch between modes and navigate between pages (Configuration, Diagnostics, and Other pages) using the buttons on the left hand side.



Device Configuration

The device configuration area is where you assign the device description, IP address, and other network parameters. Changes can only be made when the gateway is in Configuration Mode. Click the **Edit** button to make these changes.



Once you are done configuring the Description and the Network Settings, click the **Save Parameters** button.

If you are changing the IP Address of the gateway, the change will not take effect until the unit has been rebooted. After reboot, you must enter the new IP Address into the URL.

It is recommended to leave the DNS Gateway set to 0.0.0.0 and the Ethernet Link as Auto-Negotiate. If configuring the gateway to use E-mail, the DNS Gateway must be set.

Modbus TCP/IP Server Configuration

Click the **Modbus TCP/IP Server** button to access the configuration page.

1) Enter a **Device Label** to identify the device within the gateway.

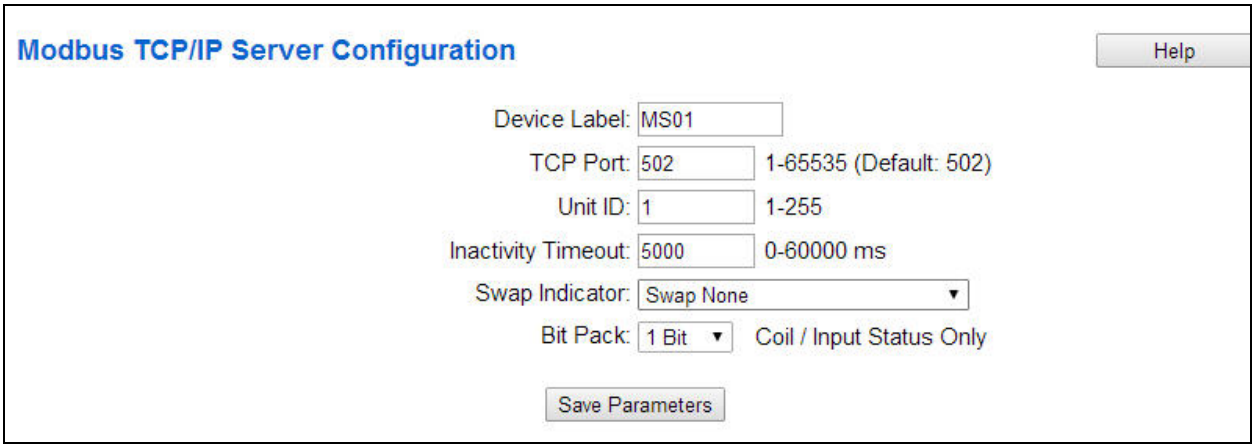
2) **TCP Port**: Enter in a TCP Port for the Modbus TCP Server to listen on. Default for Modbus TCP/IP is 502.

3) **Unit ID**: This Unit ID must be unique for all Modbus TCP Server devices on the TCP network.

4) **Inactivity Timeout**: Amount of time the gateway will wait for a read/write request before issuing a timeout.

5) To enable data swapping, select the required **Swap Indicator**. If the bytes appear in the wrong order, enable swapping to change the data. This swapping does *NOT* change Coils and their ordering inside the Bit Pack.

6) **Bit Pack**: Select the formatting of the Coil Status/Input Status. Automap will use this packing size to map coils to/from the other protocol. The bit pack selection here should match that of the other protocol. The starting address is considered Bit 0 and is the low-order bit.


Modbus TCP/IP Server Configuration
Help
Device Label: MS01
TCP Port: 502 1-65535 (Default: 502)
Unit ID: 1 1-255
Inactivity Timeout: 5000 0-60000 ms
Swap Indicator: Swap None
Bit Pack: 1 Bit Coil / Input Status Only
Save Parameters

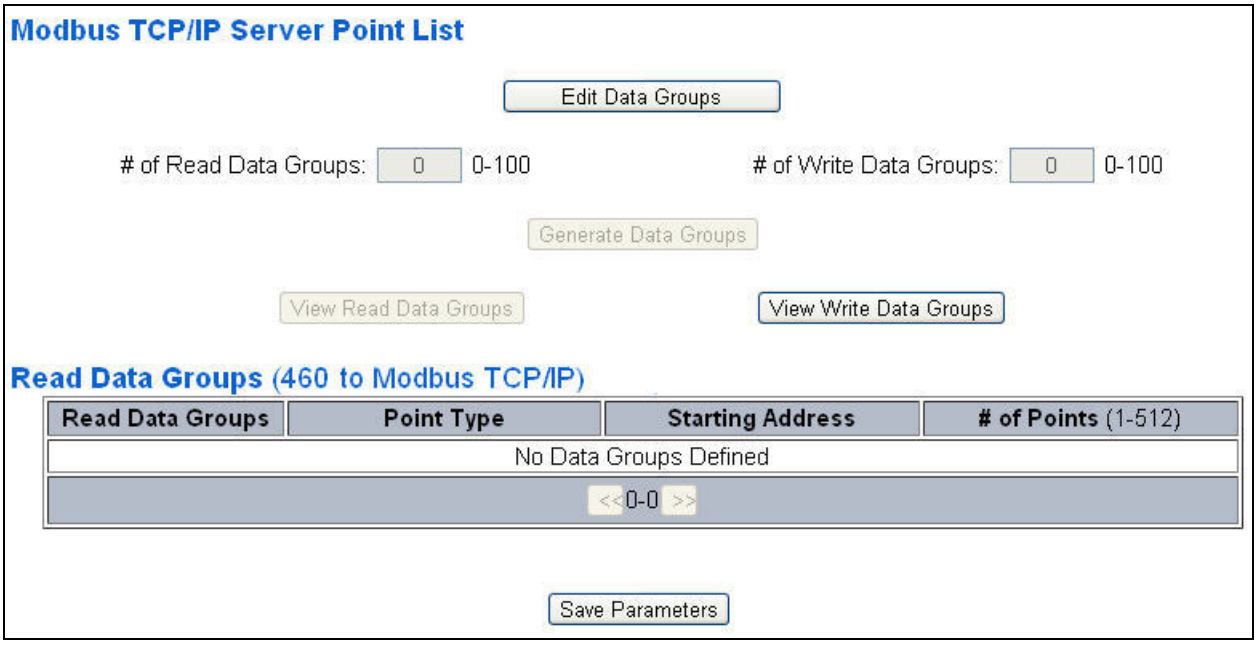
Modbus TCP/IP Server Configuration-Data Groups

The bottom area of the Modbus TCP/IP Server Configuration page lets you configure up to 100 Data Groups for both the Read/Write.

There are two ways to configure this protocol:

- Auto-Server Mode(Default)
- Manual Mode

NOTE: You may go back and forth between modes, but when reverting from Manual Mode to Auto-Server Mode, all changes made in Manual Mode will be discarded.



Modbus TCP/IP Server Data Group Configuration: Auto-Server Mode (Default)

While in Auto-Server mode the # of data groups and the actual data groups themselves cannot be edited. Auto- Server Mode looks at the other protocol and then configures the Data Groups to match. The Data Formats will be defined after the other protocol is configured.

The data will be configured according to the following rules:

- Any Coils, 8 Bit Signed/Unsigned, or 1/8/16/32 Bit Binary Packs data will be mapped as **0x Coil Status.**
- Any 16 Bit Signed/Unsigned data will be mapped as **4x Hold Reg 16 Bit Int or 16 Bit Uint**, matching signs whenever possible.
- Any 32 Bit Signed/Unsigned data will be mapped as **4x Hold Reg 32 Bit Int or 32 Bit Uint**, matching signs whenever possible.
- Any 64 Bit Signed/Unsigned data will be mapped as **4x Hold Reg 64 Bit Int or 64 Bit Uint**, matching signs whenever possible.
- Any 32 Bit Float will be mapped as **4x Hold Reg 32 Bit Float**.
- Any 64 Bit Float will be mapped as **4x Hold Reg 64 Bit Float**.
- Any String Data Types will be mapped as **4x Hold Reg String**.
- The Read or Write direction depends on whether it is configured as a Read or Write on the other protocol.
- If the other protocol exceeds the number of Data Groups supported, then nothing will be mapped. You will see the # of Data Groups remain at 0 and the main page will display the following error:

  - To fix this error, simply decrease the amount of data you configured on the other protocol so that the max number of Data Groups is not exceeded OR call customer support to increase the limits.

To add additional or edit existing Data Groups you will need to go into Manual Mode.

Modbus TCP/IP Server Data Group Configuration: Manual Mode

1. Click the **Edit Data Groups** button to switch from Auto-Server Mode to Manual Mode. Once clicked the button will read **Auto-Configure Server**. The fields under the Data Groups can now be edited.

    a. When prompted, click **OK** to confirm mode change or **Cancel** to remain in Auto Mode.

    b. Click **OK** again to keep current Data Group settings or click **Cancel** to discard the current configuration.

2. Enter the number of Read Data Groups and Write Data groups.

3. Click the **Generate Data Groups** button to have the read and write data groups auto-generate for you. You may manually configure the read and write data groups after they have been generated.

4. Follow these steps to manually configure Read Data Groups.

    a. Select **View Read Data Groups** if not already selected.

    b. Select a **Point Type** for each Scan Line. Options include: Coil Status, Input Status, Input Registers, and Holding Registers. **Note**: Input/Holding Registers have a data type associated with them.

        - String Point Type- If the mating protocol supports strings, you may select string as a point type in Modbus. With this point type, 2 characters will be packed into a single register and the first register will be set aside for the length.

          EX: 4x Hold Reg (String) with a Starting Address of 1 for a length of 5 Registers

          This means that Register 1 will hold the length of the string and Registers 2-5 will hold the string contents. This string can contain a max of 8 characters.

    c. Enter a **Starting Address** (1-based).

    d. Enter the **# of Points** to read. This will allocate the number of the data type selected.

5. Follow these steps to manually configure Write Data Groups.

    a. Select **View Write Data Groups** if not already selected.

    b. Select a **Point Type** to configure. Options include: Coil Status and Holding Registers. **Note**: Holding Registers have a data type associated with them.

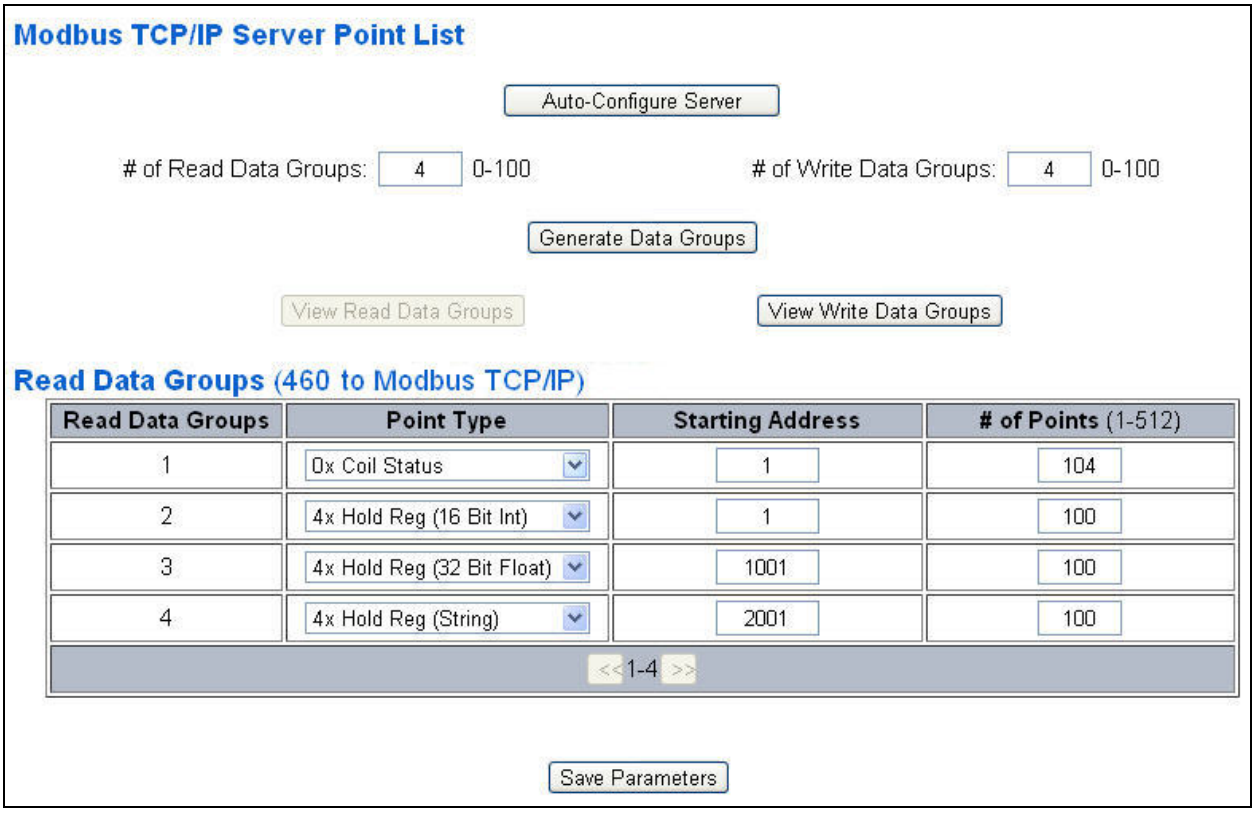
        - String Point Type- If the mating protocol supports strings, you may select string as a point type in Modbus. With this point type, 2 characters will be packed into a single register and the first register will be set aside for the length.

          EX: 4x Hold Reg (String) with a Starting Address of 1 for a length of 5 Registers

This means that Register 1 will hold the length of the string and Registers 2-5 will hold the string contents. This string can contain a max of 8 characters.

c. Enter a **Starting Address** (1-based).

d. Enter the **# of Points** to write. This will allocate the number of the data type selected.


Modbus TCP/IP Server Point List
Auto-Configure Server
# of Read Data Groups: 4 0-100
# of Write Data Groups: 4 0-100
Generate Data Groups
View Read Data Groups
View Write Data Groups
Read Data Groups (460 to Modbus TCP/IP)
Read Data Groups
Point Type
Starting Address
# of Points (1-512)
1 0x Coil Status 1 104
2 4x Hold Reg (16 Bit Int) 1 100
3 4x Hold Reg (32 Bit Float) 1001 100
4 4x Hold Reg (String) 2001 100
<< 1-4 >>
Save Parameters

BACnet/IP Server Configuration

Click the **BACnet/IP Server** button to access the primary configuration page for this device.

1) Enter a **Device Label**. This is an internal device alias used during data mapping.

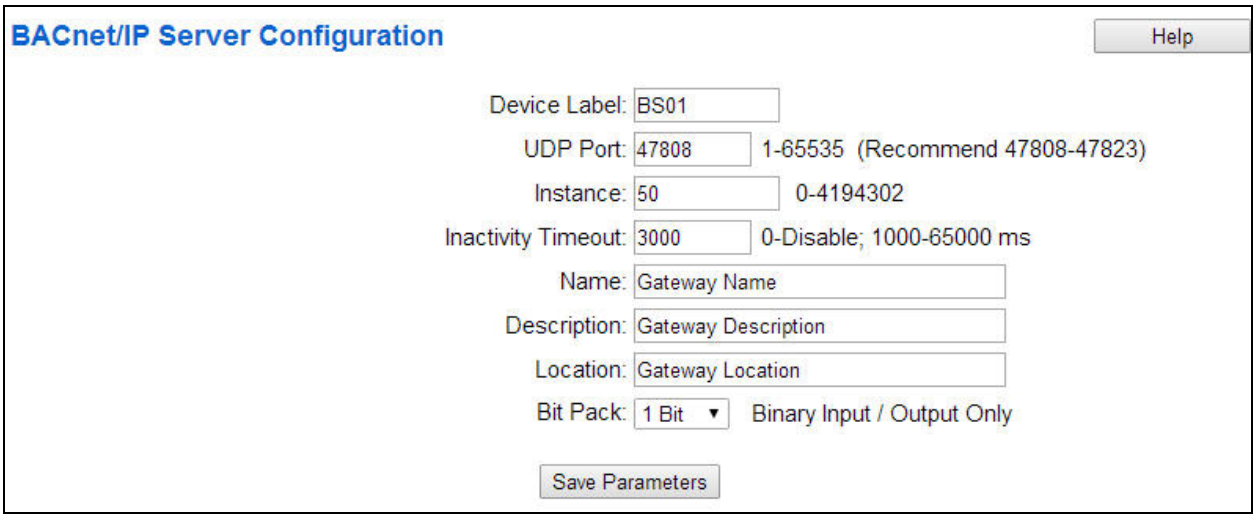
2) Enter the decimal value of the **UDP Port** that the gateway will communicate on (Default is 47808 (0xBAC0)).

3) Enter a unique **Instance** identifier for the gateway. This Instance must be unique on the BACnet/IP network.

4) **Inactivity Timeout**: Enter the amount of time, in milliseconds, the gateway should wait before a timeout state is declared. If the BACnet/IP Client does not initiate communication within this time frame the BACnet/IP LED will flash red and the timeout counter will increment. Enter 0 to disable this feature.

5) Enter a **Name**, **Description** and **Location** for the gateway. These are used to identify the gateway on the BACnet/IP network.

6) **Bit Pack**: Select the formatting of the Binary Input/Output. Automap will use this packing size to map binary objects to/from the other protocol.



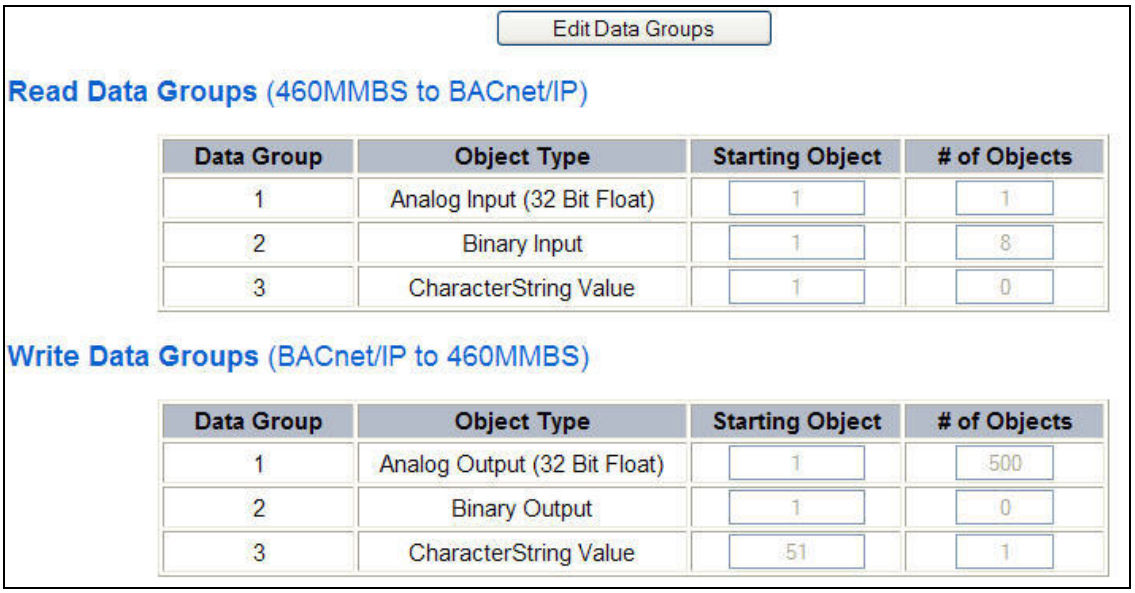
BACnet/IP Server Configuration-Data Groups

The bottom area of the BACnet/IP Server Configuration page lets you configure multiple objects for Read and Write Groups.

There are two ways to configure this protocol:

- Auto-Server Mode(Default)
- Manual Mode

NOTE: You may go back and forth between modes, but when reverting from Manual Mode to Auto-Server Mode, all changes made in Manual Mode will be discarded.



The setup in the example above will give you the following results:

- 1 AI is created with the address of AI1
- 8 BIs are created with the addresses BI1 through BI8
- 500 AOs are created with the addresses AO1 through AO500
- 1 CSV is created with the address of CSV51

BACnet/IP Server Configuration: Auto-Server Mode (Default)

While in Auto-Server mode no fields under the Data Groups can be edited. Auto-Server Mode looks at the other protocol and then configures the Data Groups below to match. BACnet/IP points and will be defined after the other protocol is configured.

Within the BACnet/IP Server, the data will automatically be configured according to the following rules:

- Any 8 Bit Signed/Unsigned, 16 Bit Signed/Unsigned, 32 Bit Signed/Unsigned, 64 Bit Signed/Unsigned, 32 Bit Float, and 64 Bit Float data will be mapped as **Analog Objects**.
- Any Coils or 1/8/16/32 Bit Binary Packs will be mapped as **Binary Objects**.
- Any String Data Types will be mapped as **CharacterString Value Objects**.
- The Input or Output Object direction depends on whether it is configured as a Read or Write on the other protocol.
- If the other protocol exceeds the number of Analog, Binary or CharacterString Value Objects the BACnet/IP Server supports (see limits on webpage), then nothing will be mapped. You will see the # of Objects column remain at 0 and the main page will display the following error:

  - To fix this error, simply decrease the amount of data you configured on the other protocol so that the max number of BACnet/IP objects is not exceeded OR call customer support to increase the limits.

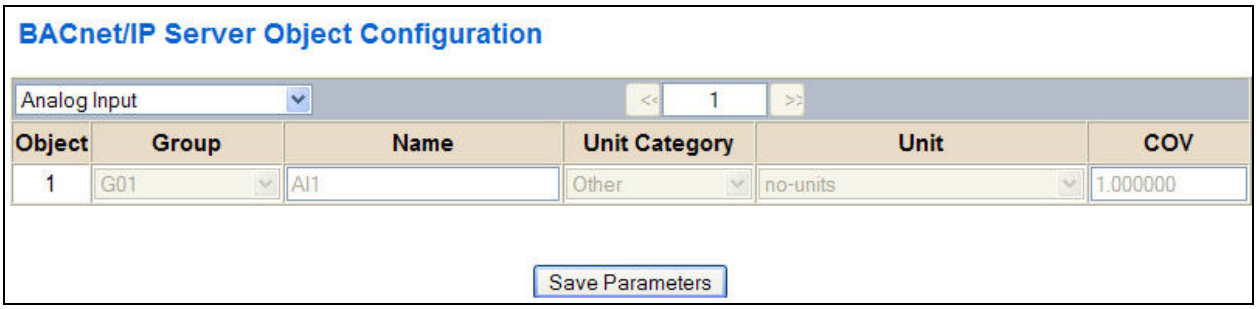
BACnet/IP Server Configuration: Manual Mode

1. Click the **Edit Data Groups** button to switch from Auto-Server Mode to Manual Mode. Once clicked the button will read **Auto-Configure Server**. The fields under the Data Groups can now be edited.
   a. When prompted, click **OK** to confirm mode change or **Cancel** to remain in Auto Mode.
   b. Click **OK** again to keep current Data Groups and Object Properties (includes any default Object Names, Units, and COV) or click **Cancel** to discard the current configuration.
2. For each object type in the Read and Write Data Groups sections, select the number of objects that the Server will support.
3. Each object has its starting object number sequentially identified at 1. This field may be modified.
4. When done, click the **Save Parameters** button.

BACnet/IP Server Object Configuration – Analog Objects

Click the **Set Up BACnet Names, Units, and COV** button at the bottom of the BACnet/IP Server Configuration page to access the Object Configuration page.

When in Auto-Server Mode, these fields are not configurable.



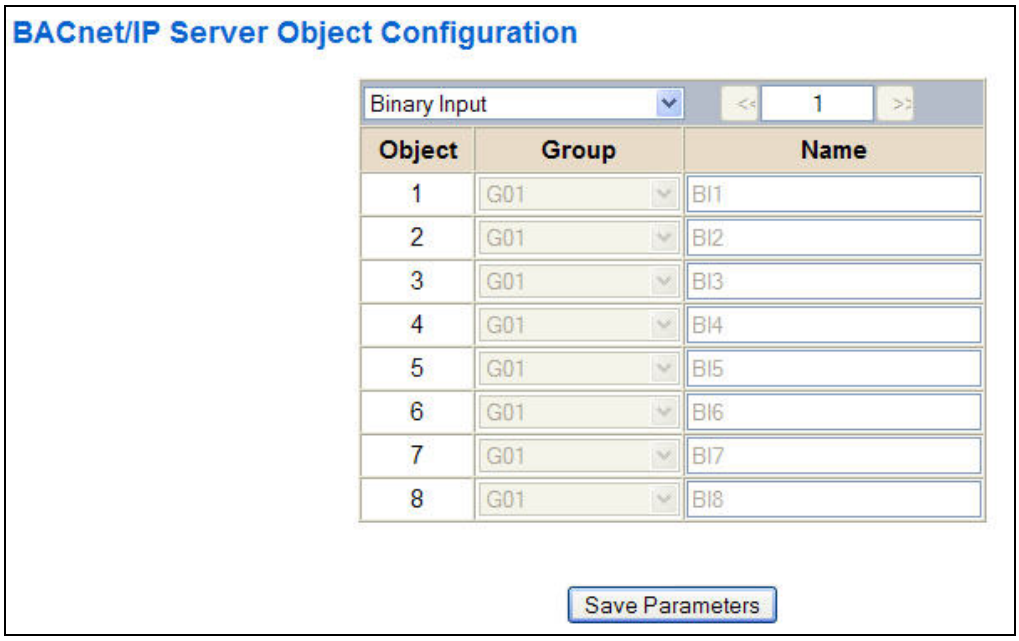
Follow these steps to customize Analog Inputs or Outputs in Manual Mode.

1) Select **Analog Input** or **Analog Output** from the upper left dropdown menu.
2) Select a **Group** to use.
    - These group names are defined in this under BACnet Advanced configuration.
3) Enter a **Name** to identify this object on the network.
    - The combination of **Group** and **Name** should be unique for each point in the gateway.
4) Select the **Unit Category** corresponding to the units you want this object to be identified with (optional). Then select the **Unit** from the dropdown menu.
5) Set the **COV** (Change Of Value) for this object.
    - If the BACnet/IP Client issues a COV-Subscription, the gateway will issue a COV Notification when the Present-Value changes by more than the given COV-Value. This value shift can be in a positive or negative direction.

BACnet/IP Server Object Configuration – Binary Objects

Click the **Set Up BACnet Names, Units, and COV** button at the bottom of the BACnet/IP Server Configuration page to access the Object Configuration page for this device.

When in Auto-Server Mode, these fields are not configurable.



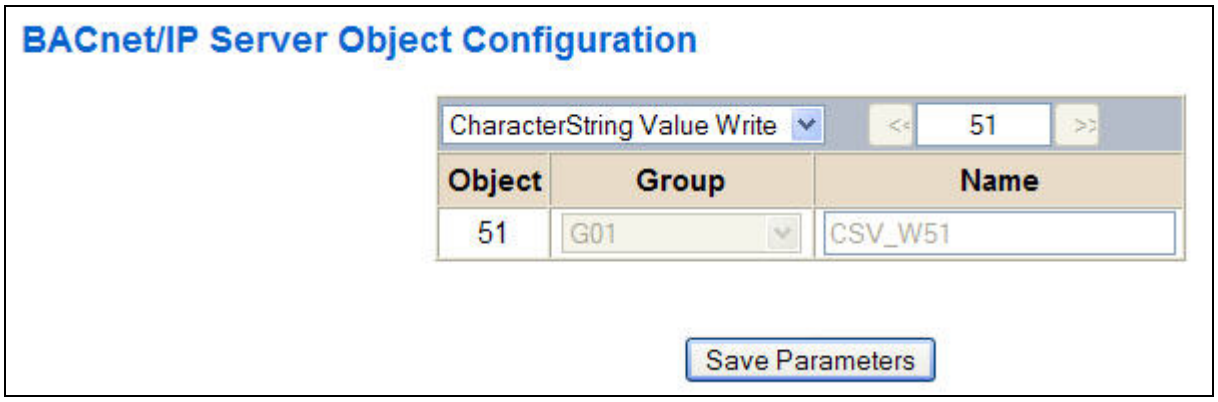
Follow these steps to configure Binary Input or Outputs in Manual Mode.

1) Select **Binary Input** or **Binary Output** from the upper left dropdown menu.
2) Select a **Group** to use.
    - These group names are defined in this under BACnet Advanced configuration.
3) Enter a **Name** to identify this object on the network.
    - The combination of **Group** and **Name** should be unique for each point in the gateway.

BACnet/IP Server Object Configuration – CharacterString Value Objects

Click the **Set Up BACnet Names, Units, and COV** button at the bottom of the BACnet/IP Server Configuration page to access the Object Configuration page for this device.

When in Auto-Server Mode, these fields are not configurable.



Follow these steps to configure Binary Inputs or Outputs in Manual Mode.

1) Select **CharacterString Value Read** or **CharacterString Value Write** from the upper left dropdown menu.

2) Select a **Group** to use.

   - These group names are defined in this under BACnet Advanced configuration.

3) Enter a **Name** to identify this object on the network.

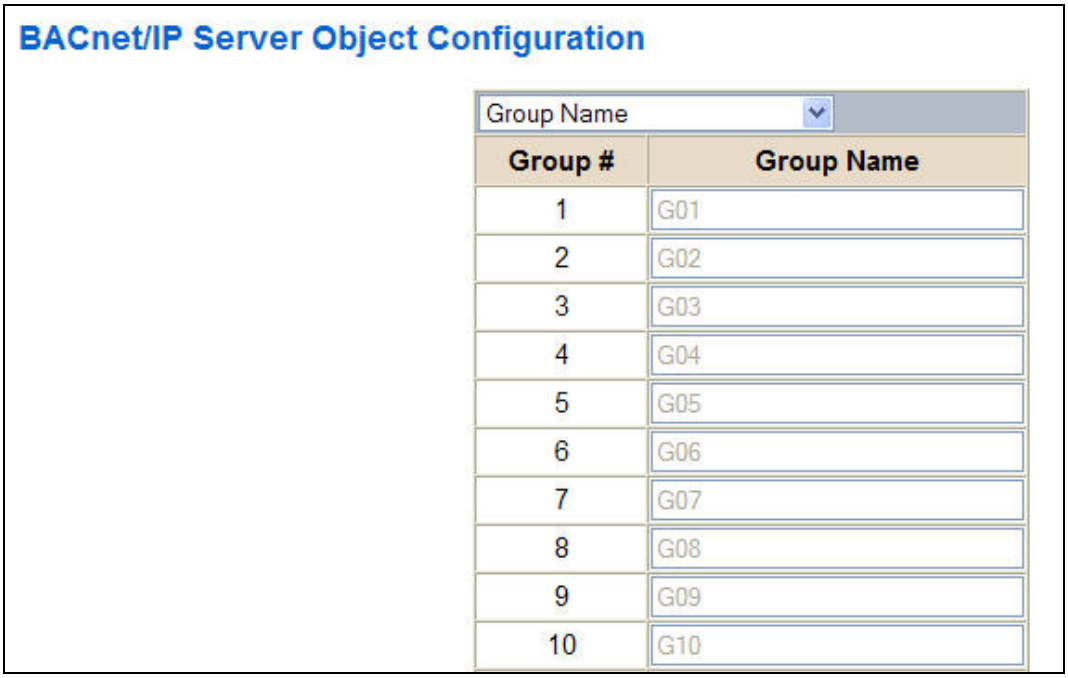
   - The combination of **Group** and **Name** should be unique for each point in the gateway.

BACnet/IP Server Object Configuration – Group Names

Click the **Set Up BACnet Names, Units, and COV** button at the bottom of the Advanced BACnet/IP Server Configuration page.

When in Auto-Server Mode, these fields are not configurable.

The **Group Name** is designed to be used when there are multiple BACnet/IP objects that have the same name. This is useful when you have multiple, identical devices connected on the other protocol.



Follow these steps to configure the Groups in Manual Mode.

1) Select **Group Name** from the upper left dropdown menu.

2) For each **Group Name** used in the previous setup, change the name to your desired text. Any names not used do not need to be changed or configured.

BACnet/IP Server Routing Configuration

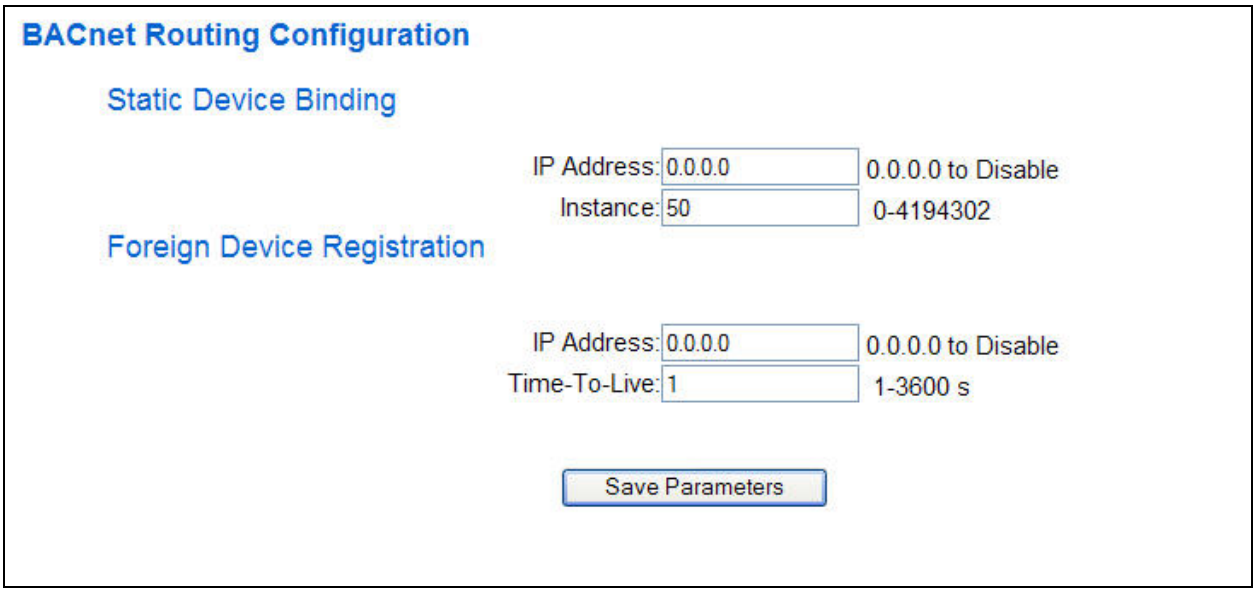
Click the **Set Up Static Device Binding and Foreign Device registration** button at the bottom of the BACnet/IP Server Configuration page to access the Routing Configuration page for this device.

These settings are used when connecting to a BACnet/IP Client on a different subnet.

There are 2 ways to cross subnets on BACnet/IP:

1) Foreign Device Registration (Recommended): This option can be used ONLY when the BBMD (BACnet/IP Broadcast Management Device) device on the other subnet (often integrated into Client devices) supports Foreign Device Registration. To use, enter the IP Address of the BBMD device into the gateway and select a Time-To-Live (TTL), the TTL defines often our gateway should send a message to the BBMD device alerting them of the gateways presence.

2) Static Device Binding: This option can be used only if the BACnet/IP Client supports Static Device Binding. This typically isn't supported. To use, simply enter the IP Address and Device Instance of the Client device. The Client device will have to enter the IP Address and Device Instance of our gateway as well.



Mapping - Transferring Data between Devices

There are 5 ways to move data from one protocol to the other. You can combine any of the following options to customize your gateway as needed.

Option 1 – Data Auto-Map: The gateway will automatically take the data type (excluding strings) from one protocol and look for the same data type defined in the other protocol. If there isn't a matching data type, the gateway will map the data to the largest available data type. See Data Auto-Map section for more details.

Option 2 – String Auto-Map: The gateway will automatically take the string data type from one protocol and map it into the other. See String Auto-Map section for more details.

Option 3 – Manual Map: If you don't want to use the Auto-Map function, you must use the manual mapping feature to configure translations.

Option 4 – Manipulation/Scaling: You can customize your data by using math operations, scaling, or bit manipulation. See Data Mapping-Explanation section for more details.

Option 5 – Move Diagnostic Information: You can manually move diagnostic information from the gateway to either protocol. Diagnostic Information is not mapped in Auto-Map mode. See Diagnostic Info section for more details.

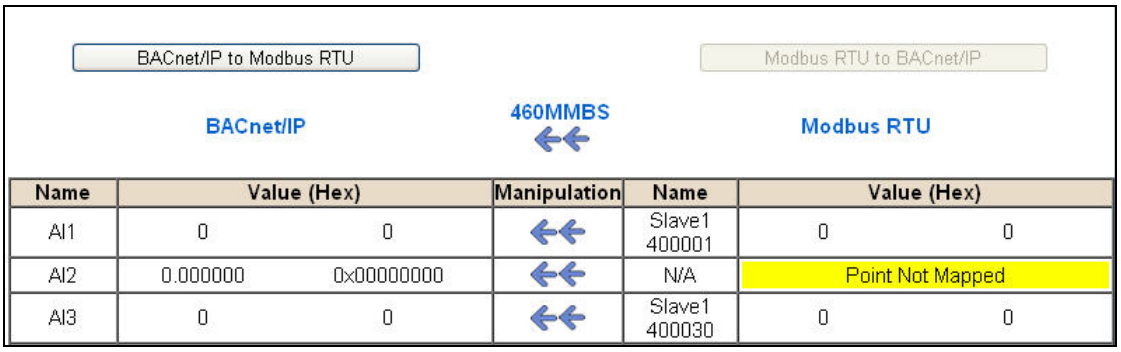
Display Mapping and Values

The Display Data and Display String pages are where you can view the actual data for each mapping that is set up.

Display Data

Click the **Display Data** button to view how the data is mapped and what the values of each mapping are. Here you will see how each data point (excluding strings) is mapped. To view, select the device from the dropdown menu and click **View** to generate the information regarding that device. Then select either the ***Protocol 1 to Protocol 2*** or ***Protocol 2 to Protocol 1*** button, correlating to the direction you wish to see the data.

This page is very useful when verifying that all data is mapped somehow from one protocol to another. If a data point is not mapped, it will display on this page in a yellow highlighted box.



Name	Value (Hex)		Manipulation	Name	Value (Hex)	
AI1	0	0	⇐⇐	Slave1 400001	0	0
AI2	0.000000	0x00000000	⇐⇐	N/A	Point Not Mapped	
AI3	0	0	⇐⇐	Slave1 400030	0	0

In the above example, we see the following:

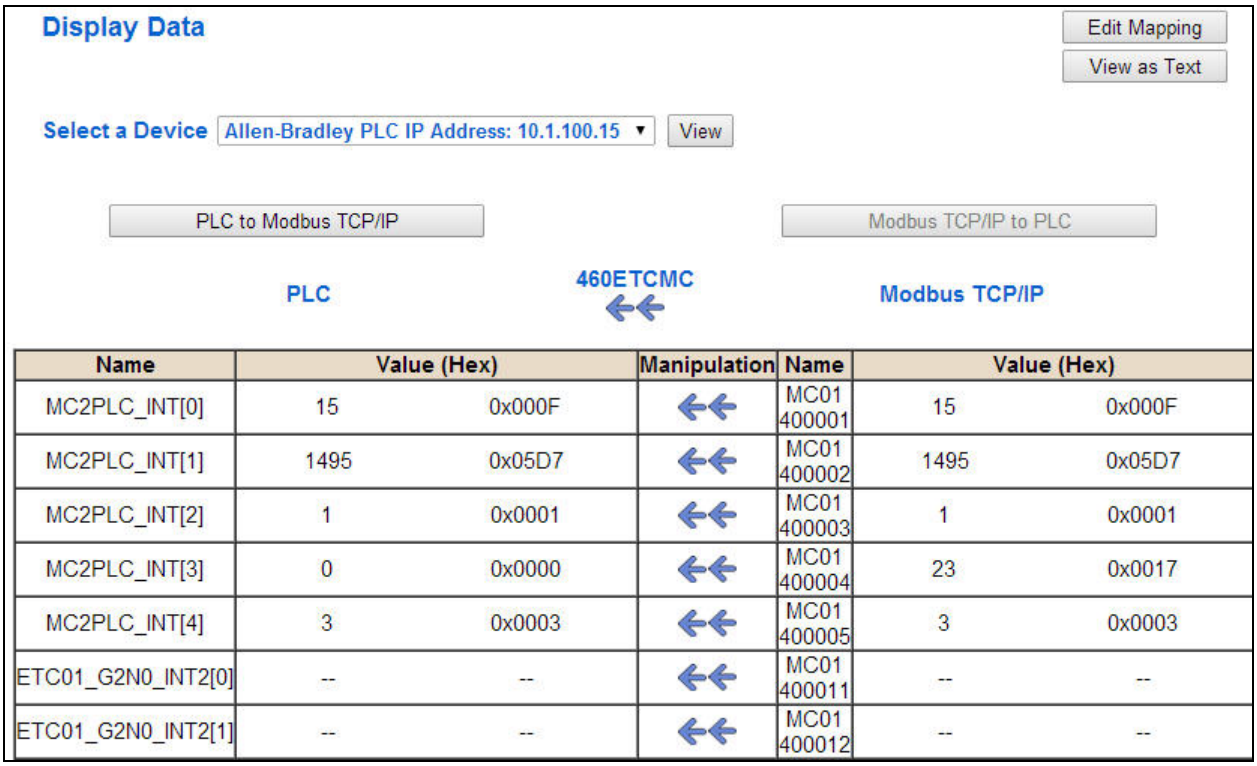
- Modbus 400001 from Slave 1 is being mapped to AI1 on BACnet
- Nothing is being moved from Modbus to AI2 on BACnet
- Modbus 400030 from Slave 1 is being mapped to AI3 on BACnet

NOTE: If a data point is mapped twice, only the first instance of it will show here. EX: If Modbus 400001 & 400040 from Slave 1 are both mapped to AI1, only 400001 will show as being mapped to AI1.

If there are values of "- -" on this page, it indicates that the source has not yet been validated and no data is being sent to the destination.

The example below reflects the Modbus to PLC flow of data. The Modbus (right side) is the source and the PLC (left side) is the destination.

- The 460 gateway has received valid responses from Modbus registers 400001-400005 and therefore can pass the data on to the PLC tag called MC2PLC_INT.
- The 460 gateway has NOT received valid responses from Modbus register 400011 & 400012. As a result, the data cannot be passed to the PLC tag ETC01_GN0_INT2 and indicates so by using "- -" in the value column of the table.



Name	Value (Hex)		Manipulation	Name	Value (Hex)	
MC2PLC_INT[0]	15	0x000F		MC01 400001	15	0x000F
MC2PLC_INT[1]	1495	0x05D7		MC01 400002	1495	0x05D7
MC2PLC_INT[2]	1	0x0001		MC01 400003	1	0x0001
MC2PLC_INT[3]	0	0x0000		MC01 400004	23	0x0017
MC2PLC_INT[4]	3	0x0003		MC01 400005	3	0x0003
ETC01_G2N0_INT2[0]	--	--		MC01 400011	--	--
ETC01_G2N0_INT2[1]	--	--		MC01 400012	--	--

To view the actual data mappings, click the **Edit Mapping** button. For more details, see the Data Mapping-Explanation section.

To view the data mappings purely as text, click the **View as Text** button. For more details, see the View Data Mapping as Text section.

Display String

Click the **Display String** button to view how the string data types are mapped and what the values of each string are. Here you will see how each string from each protocol is mapped to the other. To view, select the source or destination group and the String from the dropdown menu to generate the information regarding that device. The string data will be displayed in both hex and ASCII.

If there are values of "Data Not Valid" on this page, it indicates that the source has not been validated yet and no data is being sent to the destination.

In the example below, this page reflects the Modbus to PLC flow of data. Since the Destination "Dst: ETC01 ETC01_G2N0_STRING" displays "Data Not Valid", it can be assumed that the source field has not yet been validated.

To view the string mappings, click the **Edit Mapping** button. For more details see the String Mapping-Explanation section.

To view the string mappings purely as text, click the **View as Text** button. For more details see the View String Mapping as Text section.

Data and String Mapping – Auto-Map

The Auto-Map function looks at both of the protocols and will map the data between the two protocols as best as it can so that all data is mapped. Inputs of like data types will map to outputs of the other protocols like data types first. If a matching data type cannot be found, then the largest available data type will be used. Only when there is no other option is data truncated and mapped into a smaller data type.

If the Auto-Map function does not map the data as you want or you want to add/modify the mappings, you may do so by going into Manual-Map mode.

The following are examples of the Auto-Map function.

1) This example shows a common valid setup.

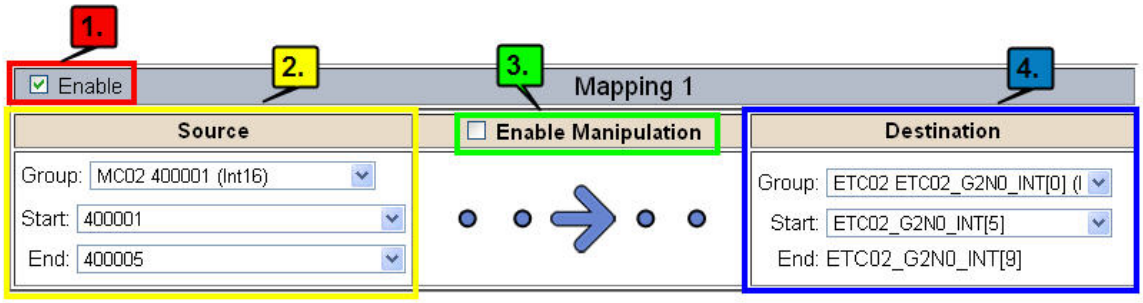
   a. Both Source values were able to be mapped to a corresponding Destination value.

2) This example shows how Auto-Map will make its best guess.

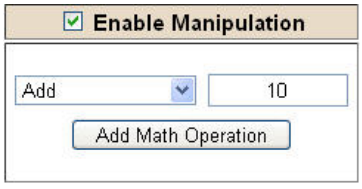
   a. The 32-bit Float from the Source location could not find a matching Destination data-type. After all other like data types were mapped, the only data type available was the 2nd 32-bit Uint data type. Auto-Map was completed even though the data in the Float will be truncated.

Data Mapping – Explanation

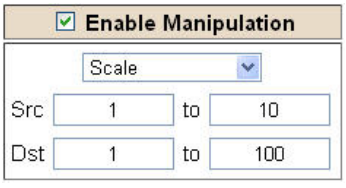
Below are the different parts that can be modified to make up a data mapping.



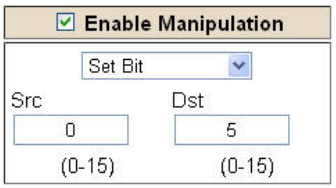
1. Enable (red box above): Check to enable mapping. If not checked, this mapping is skipped.
2. Source Field (yellow box above) :
    a. Group - Select the data group you set up in the protocol config to use for this mapping.
    b. Start - This is the starting point for this mapping.
    c. End - This is the final point to be included for this mapping.
3. Manipulation Area (green box above) :
    a. Enable the Data Manipulation. This can be enabled for any mapping.
    b. Click **Add Math Operation** for each operation needed. Up to 3 are allowed unless you are using the Scale, Set Bit, or Invert Bit functions. If using Scale, Set Bit, or Invert Bit, then only 1 operation is allowed.
    c. Select the Operation(s) to perform.
        i. Math Operations are preformed in the order they are selected.
        ii. If more than one point is selected on the source, the Math Operations will be performed on every point.
    d. Enter the value(s) for the operation.



Example of Add (similar for Subtract, Multiple, Divide, and MOD). This will add a value of 10 to the source field before it is written to the destination field.



Example of Scale. This will scale the source values from 1-10 into 1-100 for the destination.



Example of Set Bit (similar to Invert Bit). This will take the value of the 0th source bit and copy it into the value of the 5th destination bit.

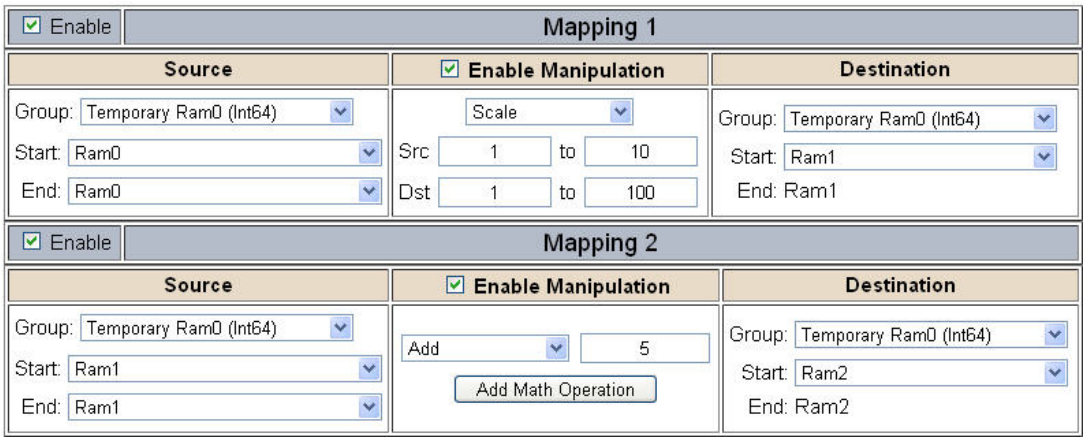
4. Destination Field (blue box above) :
    a. Group - Select the data group you set up in the protocol config to use for this mapping.
    b. Start - This is the starting point for where the data is being stored.
    c. End - The End point is derived from the length of the source and cannot be modified.

Data Mapping – Adding Diagnostic Information

Data Mapping offers 5 different types of information in addition to any scan lines specified for each protocol.

IMPORTANT NOTE: Only add Diagnostic Information **AFTER** both sides of the gateway have been configured. If changes to either protocol are made after diagnostic information has been added to the mapping table, it is necessary to verify all mappings. Remapping may be necessary.

1. Temporary Ram (Int 64)
    a. This offers five levels of 64bit Integer space to assist in multiple stages of math operations. For example, you may wish to scale and then add 5. You can set up a single translation to scale with the destination as the temporary ram. Then another translation to add 5 with the source as the temporary ram.
    b. The gateway will automatically convert the Source to fit the Destination, so there is no need for Int 8, 16, 32 since the 64 may be used for any case.



In this example, Ram0 is scaled into Ram1. Ram1 is then increased by 5 and stored into Ram2. Ram0 and Ram2 could be considered a source or destination group.

2. Temporary Ram (Double)
    a. This is similar to the Temporary Ram (Int 64), except manipulations will be conducted against the 64bit floating point to allow for large data.
3. Ticks Per Second
    a. The gateway operates at 200 ticks per second. This equates to one tick every 5ms. Thus, mapping this to a destination will give easy confirmation of data flow without involving one of the two protocols.
4. XY_NetBmpStat
    a. If a protocol is a Client/Master, there is a Network Bitmap Status that is provided. Since a Client/Master may be trying to communicate with multiple devices on the network, it

may be beneficial to know if a Server/Slave device is down. By using this Network Bitmap Status you can expose the connection statuses of individual devices.

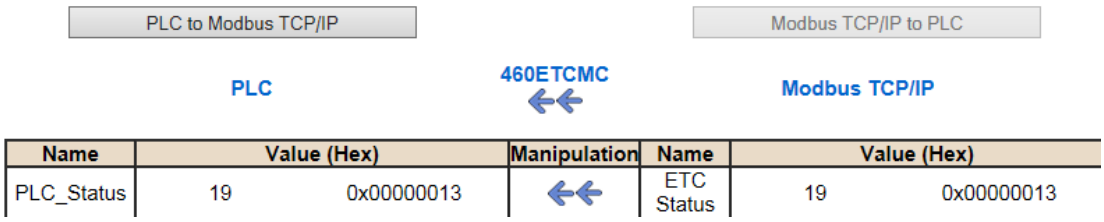
b. 0x00000002 shows that only device 2 is connected
c. 0x00000003 shows that only devices 1 and 2 are connected
d. 0x00000004 shows that only device 3 is connected

5. Status_XY
   a. There are two Statuses provided, one for each protocol. This gives access to the overall status of that Protocol. Each Bit has its own meaning as follows:

Common Status: 0x000000FF (bit 0-7)1st byte

Hex:	Bit Position:	Decimal:	Explanation:
0x00	0	0	if we are a Slave/Server
0x01	0	1	if we are a Master/Client
0x02	1	2	connected (0 not connected)
0x04	2	4	first time scan
0x08	3	8	idle (usually added to connected)
0x10	4	16	running (usually added to connected)
0x20	5	32	bit not used
0x40	6	64	recoverable fault
0x80	7	128	nonrecoverable fault

For this example the ETC Status is mapped to a PLC tag called PLC_Status



Name	Value (Hex)		Manipulation	Name	Value (Hex)	
PLC_Status	19	0x00000013		ETC Status	19	0x00000013

Example: ETC Status is 0x00000013 (19 decimal), here is the break down

Hex	Bit	Decimal	Explanation
0x01	0(on)	1	if we are a Master/Client
0x02	1(on)	2	connected (0 not connected)
0x10	4(on)	16	running (usually added to connected)
Total: 0x13		19	

External Faults: 0x0000FF00 (bit 8-15)2nd byte

Hex:	Bit Position:	Decimal:	Explanation:
0x00	8	0	local control
0x01	8	256	remotely idle
0x02	9	512	remotely faulted
0x04	10	1,024	idle due to dependency
0x08	11	2,048	faulted due to dependency

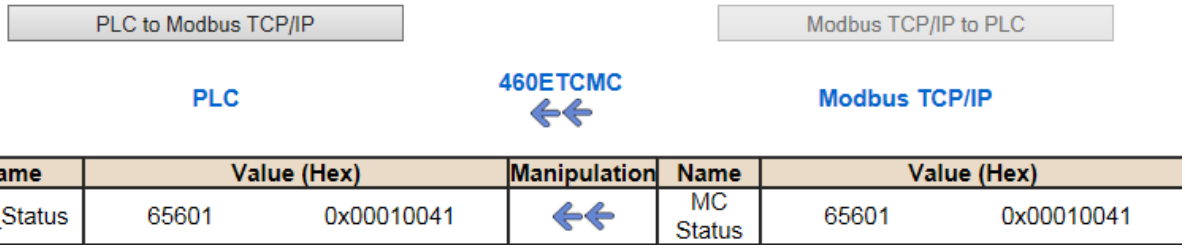
Recoverable Faults: 0x00FF0000 (bit 16-23)3rd byte

Hex:	Bit Position:	Decimal:	Explanation:
0x01	16	65,536	recoverable fault - timed out
0x02	17	131,072	recoverable fault - Slave err

Non-Recoverable Faults 0xFF000000 (bit 24-31)4th byte

Hex:	Bit Position:	Decimal:	Explanation:
0x01	24	16,777,216	nonrecoverable fault – task fatal err
0x02	25	33,554,432	nonrecoverable fault – config missing
0x04	26	67,108,864	nonrecoverable fault – bad hardware port
0x08	27	134,217,728	nonrecoverable fault – config err
0x10	28	268,435,456	Configuration Mode
0x20	29	536,870,912	No Ethernet Cable Plugged In

For this example the MC Status is mapped to a PLC tag called MC_Status



Name	Value (Hex)		Manipulation	Name	Value (Hex)	
MC_Status	65601	0x00010041		MC Status	65601	0x00010041

Example: MC Status is 0x00010041 (65601 decimal), here is the break down, we know that bytes 1 and 3 are being used, so here is the break down,

Common Status:

Hex:	Bit:	Decimal:	Explanation:
0x01	0(on)	1	if we are a Master/Client
0x40	6(on)	64	recoverable fault

Recoverable Faults:

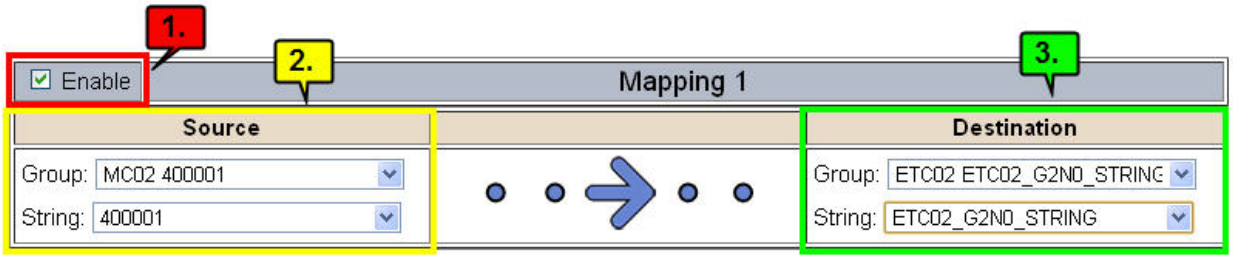
Hex:	Bit:	Decimal:	Explanation:
0x01	16	65,536	recoverable fault – timed

Total:	0x010041	65,601

String Mapping – Explanation

Below are the different parts that can be modified to make up a string mapping.

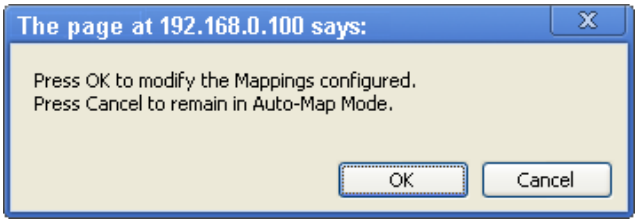
String data types can only be mapped to other string data types. There is no manipulation that can be done on the string.



1. Enable (red box above): Check to enable mapping. If not checked, this mapping is skipped.
2. Source Field (yellow box above) :
    a. Group - Select the string data group you set up in the protocol config to use for this mapping.
    b. String - This is the string used for this mapping.
3. Destination Field (green box above):
    a. Group - Select the string data group you set up in the protocol config to use for this mapping.
    b. String - This is the string where the data is being stored.

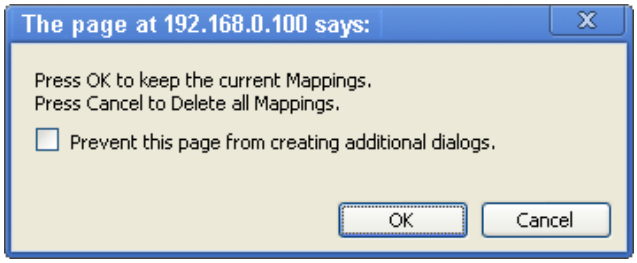
Mapping – Auto-Map Mode to Manual-Map Mode

To transition from Auto-Map mode to Manual-Map mode, click the **Edit Mapping** button. After you click this button, you will be prompted to confirm if this is really what you want to do.



Click **OK** to proceed to Manual Map mode or click **Cancel** to remain in Auto-Map mode.

There are 2 options on how to proceed from here.

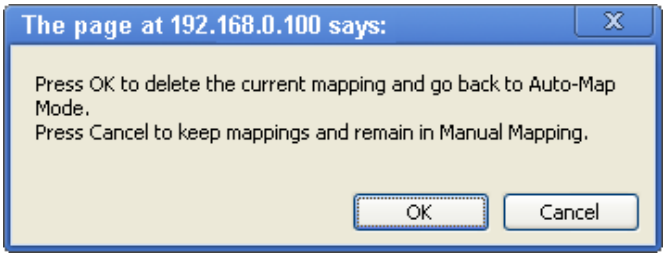

The page at 192.168.0.100 says:
Press OK to keep the current Mappings.
Press Cancel to Delete all Mappings.
Prevent this page from creating additional dialogs.
OK
Cancel

1) To keep the mappings that are already configured press **OK**.
    a. You would want this option if you are adding additional mappings or you want to modify the mapping(s) that already exist.
2) To delete the mappings that are already there and start over press **Cancel**.

To modify the number of mappings, enter a number next to **# of Mappings to Configure** and click the **Set Max # of Mappings** button. You can always add more mappings if needed.

Mapping – Manual-Map Mode to Auto-Map Mode

To transition from Manual-Map mode to Auto-Map mode, click the **Auto Map Mode** button. After you click this button, you will be prompted to confirm if this is really what you want to do.


The page at 192.168.0.100 says:
Press OK to delete the current mapping and go back to Auto-Map Mode.
Press Cancel to keep mappings and remain in Manual Mapping.
OK
Cancel

Click **OK** to proceed to delete all current mappings and go to Auto-Map mode. Click **Cancel** to keep all mappings and remain in Manual-Map mode.

NOTE: Once you revert back to Auto-Map mode there is no way to recover the mappings you lost. Any mappings you added will be deleted as well.

View Data Mapping as Text

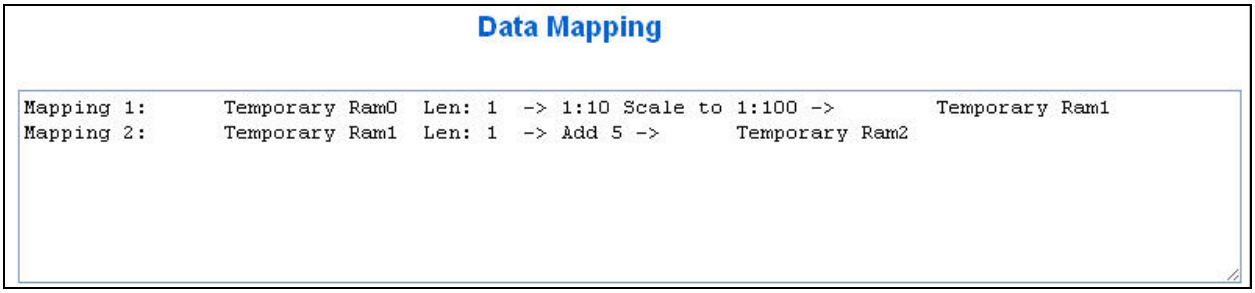
The View as Text page displays the point to point mapping(s) you set up in the Data Mapping section. This will also display any manipulation(s) that are configured.

Each line on this page will read as follows:

> **Mapping** *number***:** *source point* **Len:** *Number of points mapped* **->** *manipulation (if blank then no manipulation)* **->** *destination point*

If you are looking for a specific point to see if it is mapped, you can do a find in this text box for your point in question. Example: you defined 20 Registers starting at register 1 and want to see if 400011 is mapped. If it is not in this text box then it is not mapped and no data will be transferred.

This is the text display for the example shown under the *Data Mapping- Adding Diagnostic Information* section.


Data Mapping
Mapping 1: Temporary Ram0 Len: 1 -> 1:10 Scale to 1:100 -> Temporary Ram1
Mapping 2: Temporary Ram1 Len: 1 -> Add 5 -> Temporary Ram2

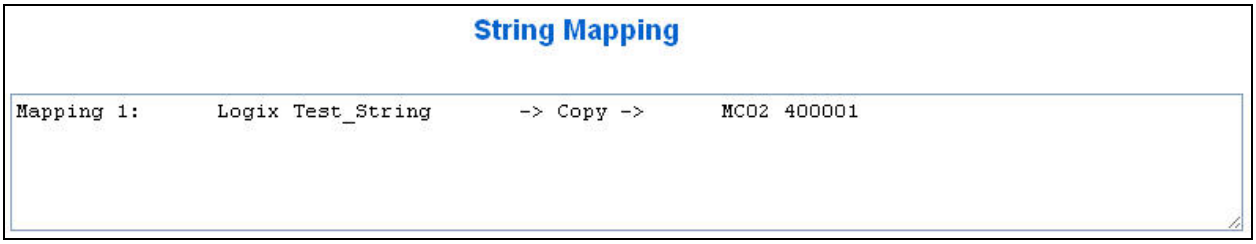
View String Mapping as Text

The View as Text page displays the string mapping(s) you set up in the String Mapping section.

Each line on this page will read as follows:

Mapping *number***:** *source point* **-> Copy ->** *destination point*

If you are looking for a specific point to see if it is mapped, you can do a find in this text box for your point in question. Example: you defined 20 String Tags in the PLC and want to see if "Test_String" in the Logix PLC is mapped. If it is not in this text box, then it is not mapped, and no data will be transferred.



Security Configuration

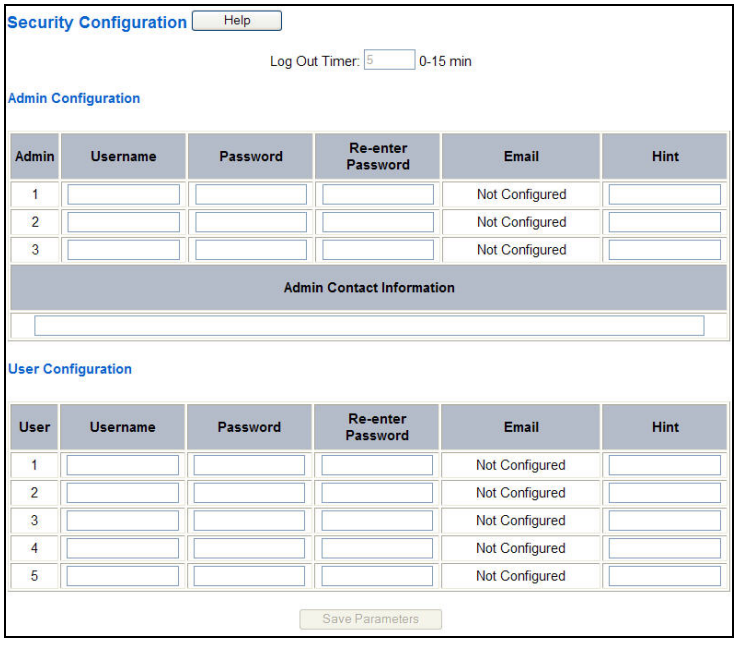
You can configure Security for 3 administrators, 5 users, and 1 guest.

THIS IS NOT A TOTAL SECURITY FEATURE

The security feature offers a way to password protect access to diagnostics and configuration on the network. The security feature does not protect against "Air Gap" threats. If the gateway can be physically accessed, security can be reset. All security can be disabled if physical contact can be made. From the login page, you would click the **Reset Password** button twice and be forced to do a hard reboot (power down) on the gateway within 15 minutes of clicking the button. This process should be used in the event a password is forgotten.

Note: Only Admins have configuration access to all web pages.

1. Log Out Timer: The system will automatically log inactive users off after this period of time. **NOTE**: A time of 0 means that the user will not be automatically logged off. Instead, they must manually click the "Logout" button.
2. Username: Enter a username, max of 32 characters.
3. Password: Enter a password for the username, max of 32 characters, case sensitive.
    a. Re-enter the Password
4. E-mail: In case the password was forgotten, a user can have their password e-mailed to them if e-mail was configured.
5. Hint: A helpful reminder of what the password is.



Security Configuration-Security Levels

Each webpage in our gateway can have a separate security level associated with it for each user.

Security Levels:

1. **Full Access**: Capability to view and configure a web page.
2. **View Access**: Capability to view a web page, but cannot configure parameters.
3. **No Access**: No capability of viewing the web page and page will be removed from Navigation.

Security - Log In

Username: Name of the user to login.

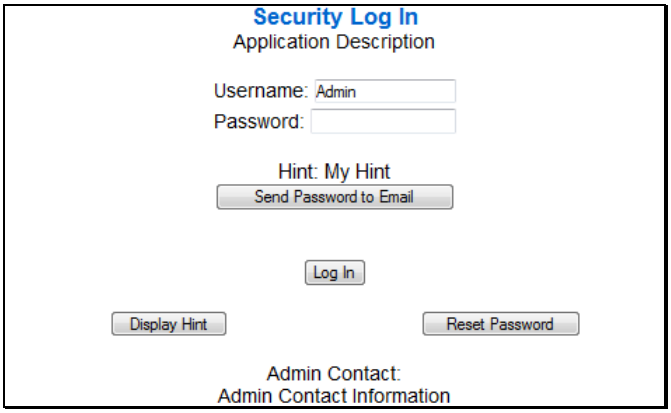
Password: Password of the user to login.

Log In: If login is successful, the user will be redirected to the Main Page.

Send Password to Email: Sends the specified User's Password to the email configured for that user.

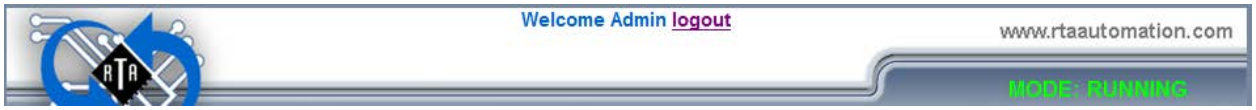
Display Hint: Displays the hint specified for the User if one was set up.

Reset Password: This is used to reset security settings. Confirm reset password must be selected to confirm this action. Once confirmed, there is a 15 minute window to do a hard reset of the gateway by physically removing and restoring power from the gateway. Once power is restored, you may navigate to the IP address of the gateway as normal.



Security - Log Out

Once a user is done with a session they may click **logout** at the top of any page. The user may also be logged out for inactivity based off of the Log Out Timer specified during the configuration.



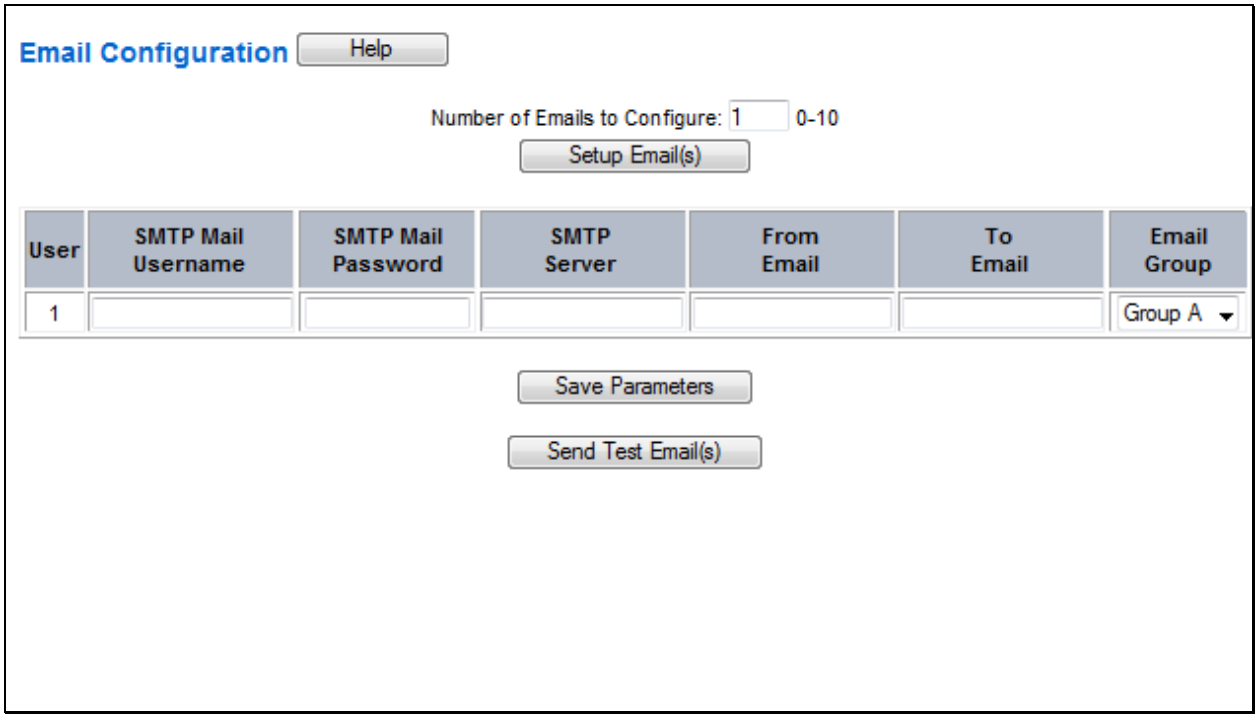
Closing the browser is not sufficient to log out.

Email Configuration

You can configure up to 10 email addresses.

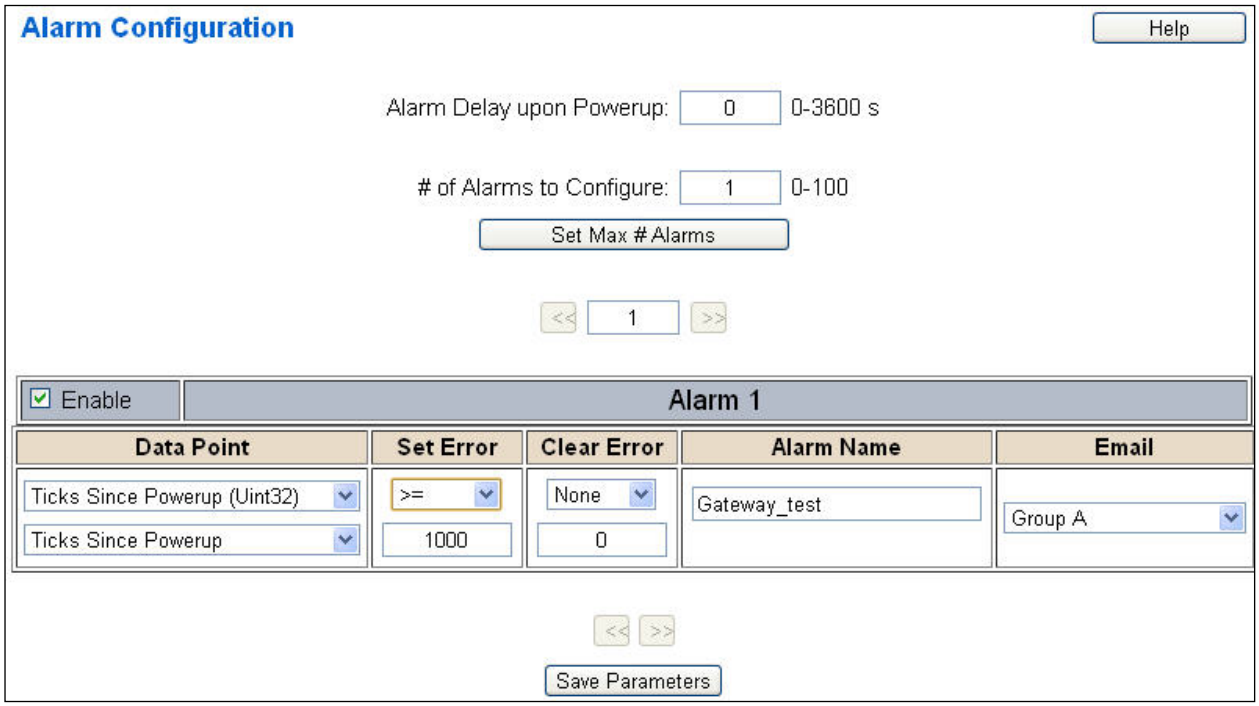
1. SMTP Mail Username: The email address that the smtp server has set up to use.
2. SMTP Mail Password: If authentication is required, enter the smtp Server's password (Optional).
3. SMTP Server: Enter the Name of the SMTP Server or the IP Address of the Server.
4. From E-mail: Enter the e-mail that will show up as the sender.
5. To E-mail: Enter the e-mail that is to receive the e-mail.
6. E-mail Group: Choose a group for the user. This is used in other web pages.

Click the **Save Parameters** button to commit the changes and reboot the gateway.



Alarm Configuration

1. Alarm Delay upon Powerup: At Powerup, the gateway will have values of '0' stored for all data. This may cause alarms to trigger before these values are updated by the mating protocols. Set this field to provide needed time to update fields before considering values for alarms.



2. Enter the number of alarms to configure and click **Set Max # Alarms** to generate those lines.
3. In the Data Point Section:
    a. Top dropdown: select the Data Group. This dropdown menu will contain all groups that go from the gateway to the network.
    b. Lower dropdown: select the Data Point's Specific Point. This is used to select which point in the group will be monitored for alarms.
4. In the Set Error Section:
    a. Select the Set Error Operation in the top dropdown menu. Available options are <, >, <=, >=, !=, ==, and Change of State (COS). This is the operation that will be used to compare the Data Point value against the Error Value to determine if the alarm needs to be set.
    b. Select the Set Error Value. This value is used as: 'Data Point's Value' 'Operation' 'Value.' Ex: Ticks Since Powerup >= 1000. This will set the alarm after 1000 ticks have elapsed since the unit powered up.

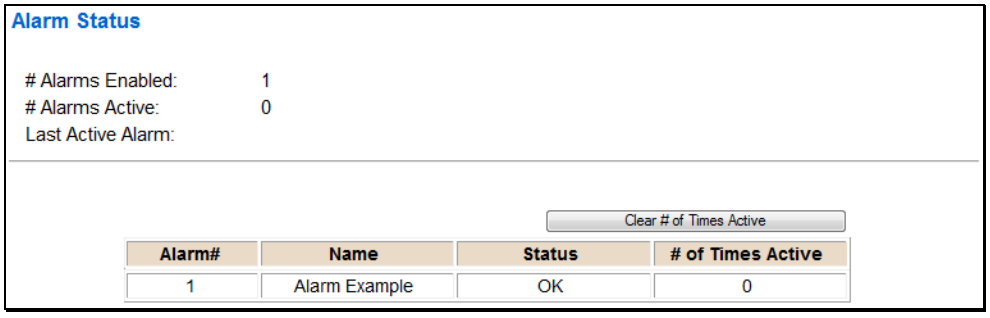
5. In the Clear Error Section:
    a. Select the Clear Error Operation. Available options are <, >, <=, >=, !=, ==, and Change of State (COS). This is the operation that will be used to compare the Data Point value against the Error Value to determine if the alarm needs to be cleared.
    b. Select the Clear Error Value.
    -Ex: Ticks Since Powerup >= 5000. This will clear the alarm after 5000 ticks have elapsed since the unit powered up.
6. Enter an Alarm Name. This will make the alarm unique and will be available in the Alarm Status page as well as in the email generated by the alarm.
7. Select an email to associate this alarm with. When an alarm is set, it sends an email. When an alarm is cleared, it will also send an email.

Click the **Save Parameters** button to commit the changes to memory and reboot the gateway.

Diagnostics – Alarm Status

Alarm Status will only display under the Diagnostic menu tab if at least 1 Alarm is enabled.

1. # Alarms Enabled: This is a count of enabled alarms.
2. # Alarms Active: This is how many alarms are presently active (set).
3. Last Active Alarm: This is the last alarm that the gateway detected.
4. **Clear # of Times Active**: This will reset all alarms '# of Times Active' to 0.
5. Alarm #: The reference number to the given alarm on the alarm setup page.
6. Name: The name of the alarm.
7. Status: The current status of the alarm, either OK or ALARM.
8. # of Times Active: This count represents the number of times this alarm has become active. If an alarm is triggered, this count will increment.

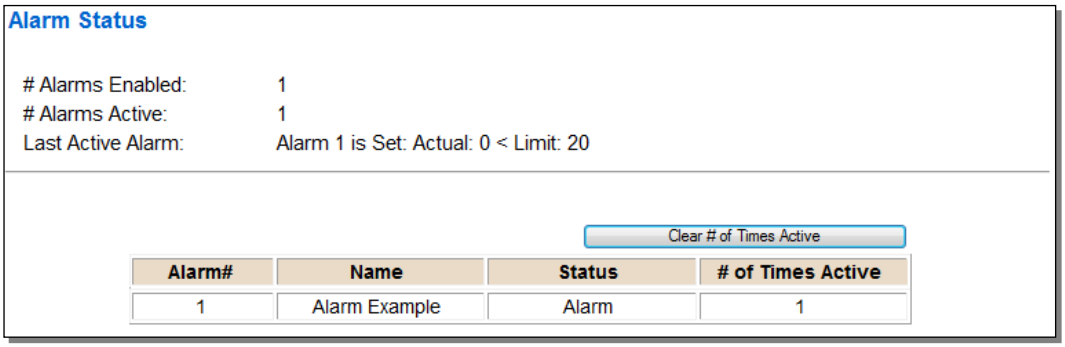

Alarm Status
Alarms Enabled: 1
Alarms Active: 0
Last Active Alarm:
Clear # of Times Active
Alarm# Name Status # of Times Active
1 Alarm Example OK 0

Alarms – Active

While one or more alarms are active, every page will display 'Alarms Active' at the top of the page. This will no longer be displayed if all active alarms have been cleared.

When an alarm is activated, the following will occur:

1. A one-time notification will be sent out to the email associated with the alarm.
    a. For duplicate emails to occur, the alarm must be cleared and then become active again.
2. *# Alarms Active* and *# of Times Active* will be incremented.
3. Status of the Individual Alarm will be set to *Alarm*.
4. *Last Active Alarm* field will be populated with details on what triggered the alarm.


Alarm Status
Alarms Enabled: 1
Alarms Active: 1
Last Active Alarm: Alarm 1 is Set: Actual: 0 < Limit: 20
Clear # of Times Active
Alarm# Name Status # of Times Active
1 Alarm Example Alarm 1

Alarms – Clear

When an alarm is cleared, the following will occur:

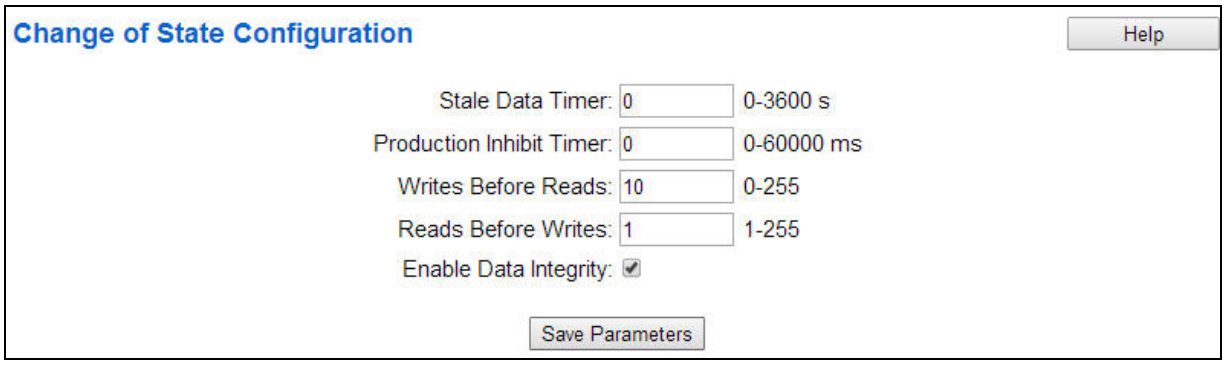
1. A one-time notification will be sent to the email associated with the alarm.
    a. For duplicate emails to occur, the alarm must become active and then be cleared again.
2. Total *# Alarms Active* will decrement. *Last Active Alarm* will not be changed.
3. Status of the Individual Alarm will be reset to *OK*.

Change of State (COS) Configuration

The gateway, by default only writes when data has changed. The gateway also waits to write any data to the destination until the source protocol is successfully connected.

Default values should fit most applications. Change these values with caution as they affect performance.

1. **Stale Data Timer**: If the data has not changed within the time allocated in this Stale Data Timer, the data will be marked as stale within the gateway and will force a write request to occur. This timer is to be used to force cyclic updates in the gateway, since data will only be written if it has changed by default. There is a separate timer per data mapping.
   Gateway behavior:
   If time = 0s => (DEFAULT) The gateway will write out new values on a Change of State basis.
   If time > 0s => The gateway will write out new values whenever the timer expires to force Cyclic updates (write every *x* seconds).
2. **Production Inhibit Timer:** Amount of time after a Change of State write request has occurred before allowing a new Change of State to be written. This is to be used to prevent jitter. Default value is 0ms. This timer takes priority over the Stale Data Timer. There is a separate timer per data mapping. This timer is active only after the first write goes out and the first COS event occurs.
3. **Writes Before Reads**: If multiple writes are queued, execute # of Writes Before Reads before the next read occurs. Default is 10 and should fit most applications. **Warning:** A value of 0 here may starve reads if a lot of writes are queued. This may be useful in applications where a burst of writes may occur and you want to guarantee they all go out before the next set of reads begin.
4. **Reads Before Writes:** If multiple writes are queued, the # of Writes Before Reads will occur before starting the # of Reads Before Writes. Once the # of Reads Before Writes has occurred, the counter for both reads and write will be reset. Default is 1 and should fit most applications.
5. **Enable Data Integrity**: If enabled, do not execute any write requests to the destination until the source data point is connected and communicating. This prevents writes of 0 upon power up.


Change of State Configuration
Help
Stale Data Timer: 0 0-3600 s
Production Inhibit Timer: 0 0-60000 ms
Writes Before Reads: 10 0-255
Reads Before Writes: 1 1-255
Enable Data Integrity:
Save Parameters

Click the **Save Parameters** button to commit the changes to memory and reboot the gateway.

Diagnostics Info

The Diagnostic page is where you will be able view the gateway's translations and protocol specific status information.

For protocol specific diagnostic information, refer to the next three pages.

Diagnostics – Data and String Mapping

The Diagnostics->Diagnostic Info->System section displays the number of translations that are enabled, for both Data and String data types, the number of mappings that have an error, and the first mapping that has an error.

 # Enabled: Number of mappings that are enabled.

 # Error: The number of mappings that are enabled that have an error.

First Error: This is a detailed description of the first mapping that has an error.

Common Errors:

1. Destination or Source Point does not exist
   -Solution: Re-map the mapping
2. Source or Destination Pointer too small
   - There is not enough space on either the Source, or the Destination for the data you want to copy. This is typically seen when the Destination is smaller than the amount of data being transferred to it.
3. Range Discard, Min or Max Value
   - The actual data value is outside of the defined range
4. Math Error
   - Operation value cannot be 0
5. Scaling Error
   - Source Min must be smaller than Source Max
   - Destination Min must be smaller than Destination Max

Diagnostics – Modbus TCP/IP Server

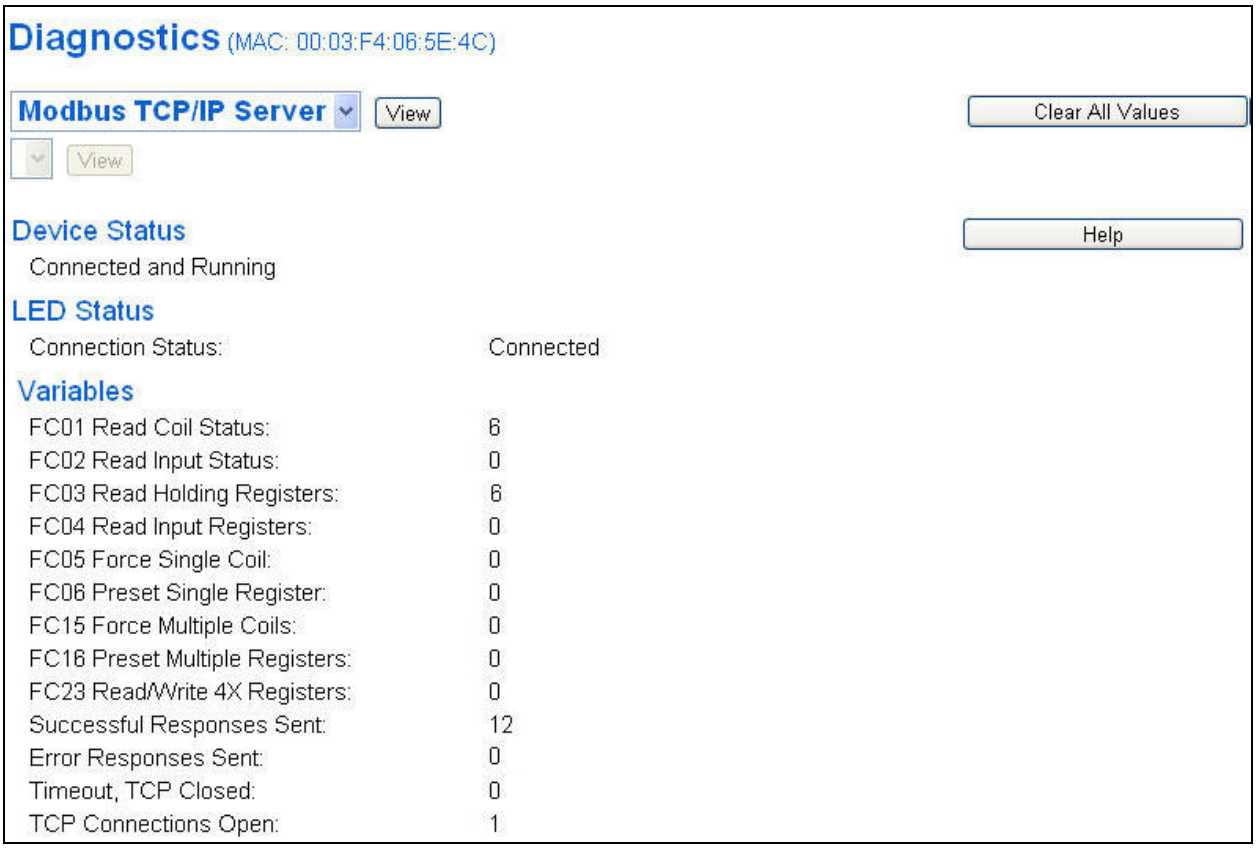
Select the **Modbus TCP/IP Server** in the dropdown menu on the Diagnostic. Additional diagnostic information can be found by clicking on the **Help** button.

Clear All Values - *This will only affect Displayed Values.*

1. This will return all values displayed to 0 and clear the status string.
2. If Viewing Modbus TCP/IP Server, this will only clear the values for the Modbus TCP/IP Server section of the gateway.

Device Status

1. Connected - A Modbus TCP/IP Client has a connection for the gateway.
2. Not Connected:
    a. Ethernet Cable not plugged in.
    b. The Modbus TCP/IP Client has not opened up communication to the gateway.
    c. The Modbus TCP/IP Client has not communicated to the gateway in "x" milliseconds, where "x" is the inactivity timeout specified in the Modbus TCP/IP Server Configuration.



Diagnostics – Modbus TCP/IP Server

LED Status:

1. Good Communication (Solid Green) – The gateway is connected to a Modbus TCP/IP Client and communicating as expected.
2. Not Connected (Flashing Green) – The Modbus TCP/IP Client has never attempted to open up communication to the gateway.
3. Connection Timeout (Flashing Red) - The gateway has lost a connection to the Modbus TCP/IP Client.
4. Off:
    a. No Power.
    b. No Ethernet cable plugged in.

Variables:

1. FC01 Read Coil Status – Modbus Function Code 1: Number of Read Coil Status requests received.
2. FC02 Read Input Status – Modbus Function Code 2: Number of Read Input Status requests received.
3. FC03 Read Holding Registers – Modbus Function Code 3: Number of Read Holding Registers requests received.
4. FC04 Read Input Registers – Modbus Function Code 4: Number of Read Input Registers requests received.
5. FC05 Force Single Coil – Modbus Function Code 5: Number of Write Coil Status requests received.
6. FC06 Preset Single Register – Modbus Function Code 6: Number of Write Holding Register requests received.
7. FC15 Force Multiple Coils – Modbus Function Code 15: Number of Write multiple Coil Status requests received.
8. FC16 Preset Multiple Registers – Modbus Function Code 16: Number of Write multiple Holding Register requests received.
9. FC23 Read/Write 4X Register – Modbus Function Code 23: Number of Read/Write Holding Registers requests received.
10. Successful Responses Sent – Total number of Read/Write messages sent by the gateway.
11. Error Responses Sent - Total number of Read/Write errors sent by the gateway.
12. Timeouts, TCP Closed – Total number of Read/Write timeouts that cause the Modbus TCP/IP connection to close.
13. TCP Connections Open – Number of Modbus TCP/IP connections that have been opened to the gateway.

Diagnostics – BACnet/IP Server

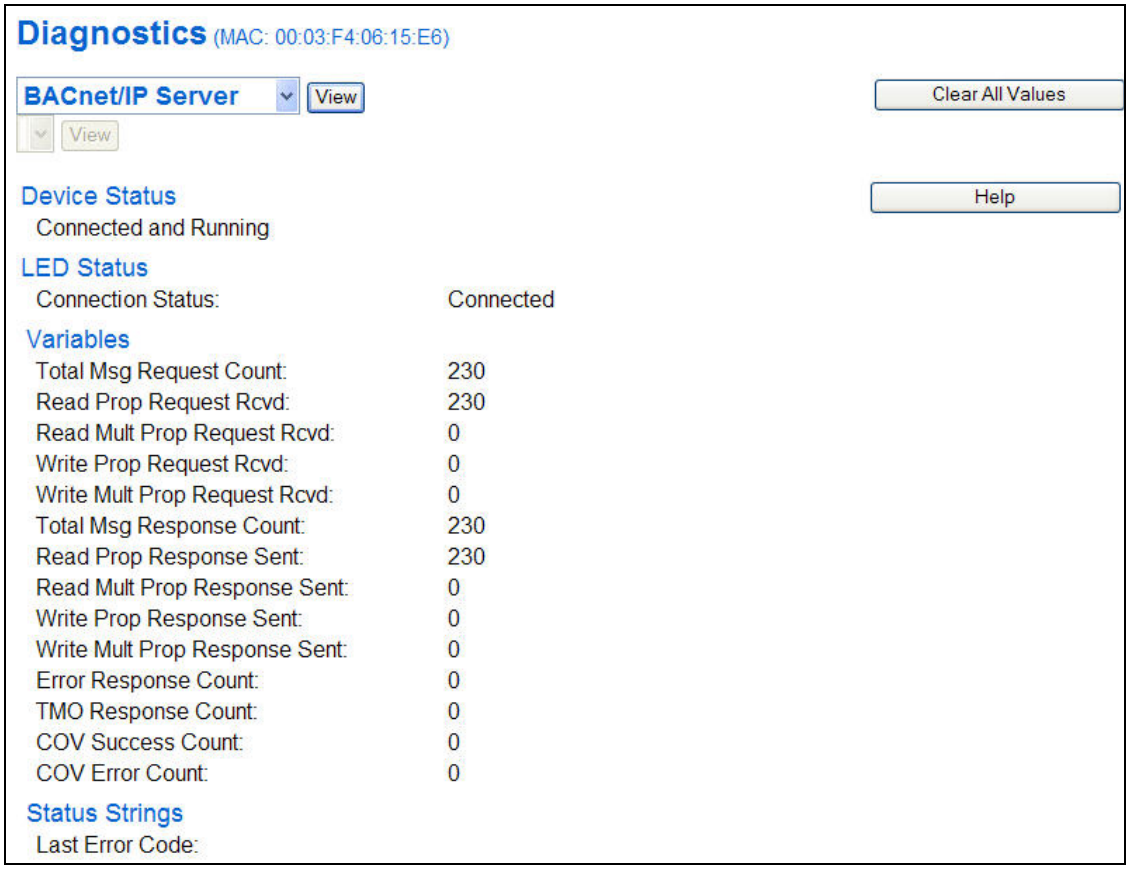
Select the **BACnet/IP Server** in the drop down menu on the Diagnostic page. Additional diagnostic information can be found by clicking on the **Help** button. Additional diagnostic information can be found by clicking on the **Help** button.

Device Status:

1. Connected – The gateway is connected to a BACnet/IP Client.
2. Not Connected – The gateway is not connected to a BACnet/IP Clients.
3. Error: Timeout –The gateway has not received a read/write request in the amount of time specified by the Inactivity Timeout.

LED Status:

1. Good Communication (Solid Green) - Connected to a BACnet/IP Client.
2. Never Connected (Blink Green) – Gateway has never been connected to a BACnet/IP Client.
3. Connection Timeout (Blink Red) –The gateway has not received a read/write request in the amount of time specified by the Inactivity Timeout.



Variables:

1. Total Msg Request Count – Total Number of Messages Received from the BACnet/IP Client.
2. Read Property Request Received – Number of Read Property requests received from the BACnet/IP Client.
3. Read Multiple Property Request Received – Number of Read Property Multiple requests received from the BACnet/IP Client.
4. Write Property Request Received – Number of Write Property requests received from the BACnet/IP Client.
5. Write Property Multiple Request Received – Number of Write Property Multiple requests received from the BACnet/IP Client.
6. Total Msg Response Count – Total Number of Messages sent to the BACnet/IP Client.
7. Read Property Response Sent- Number of Read Property Responses sent to the BACnet/IP Client.
8. Read Multiple Property Response Sent – Number of Read Property Multiple Responses sent to the BACnet/IP Client.
9. Write Property Response Sent – Number of Write Property Responses sent to the BACnet/IP Client.
10. Write Multiple Property Response Sent – Number of Write Property Multiple Responses sent to the BACnet/IP Client.
11. Error Response Count – Total Number of Read/Write Errors Received.
12. Timeout Response Count – Total Number of Read/Write Timeouts.
13. COV Success Count – Total Number of Successful COV Messages.
14. COV Error Count – Total Number of COV Error Messages.

Common Error Strings:

1. BS: UNHANDLED_MSG_TYPE – The gateway received a BACnet/IP message that it doesn't know how to process.
2. BS: Message Abort - The gateway aborted a message due to one of the common reasons below:
   a. "Buffer Overflow" – The BACnet/IP Client is asking for too much information in a single message.
   b. "Invalid ADPU" – The gateway is not able to process the message, try again later.
   c. "Preempted by Higher Priority" – The BACnet/IP Client message has aborted due to a higher priority task, try again later.
   d. "Segmentation Not Supported" – The gateway does not support segmentation. Break up the Client request into multiple requests.
3. BS: Message Reject - The gateway rejected a message due to one of the common reasons below:
   a. "Buffer Overflow" – The BACnet/IP Client is asking for too much information in a single message.
   b. "Invalid Parameter Data Type" – This BACnet/IP data type is not supported.

c. “Invalid Tag” – BACnet/IP message is not how the gateway expects the message.
d. “Parameter Out of Range” – The BACnet/IP Client is asking for information outside of the gateway's defined range.

4. BS: Message Error “XXXXX”- The gateway is sending an error a message due to the listed explanation:
   a. “Inconsistent parameters” -
      i. BACnet/IP Client tried to write a priority that was out of range or reserved (Priority 6) and was rejected.
      ii. BACnet/IP Client tried to write to ALL, REQUIRED, or OPTIONAL object property.
   b. “Invalid Data Type” – BACnet/IP Client tried to use a data type with an object that is not supported.
   c. “Service request denied” – BACnet/IP request cannot be processed at this time because the BACnet/IP connection is not established.
   d. “Read access denied” – BACnet/IP read request cannot be processed.
   e. “Unknown object” – BACnet/IP Client tried to access an object our gateway does not support.
   f. “Unknown property” – BACnet/IP Client tried to access a property our gateway does not support for that object type.
   g. “Unsupported object type” – BACnet/IP Client tried to access an object type our gateway does not support.
   h. “Value out of range” – BACnet/IP message could not be completed because the passed value was not in the valid range.
   i. “Write access denied” – BACnet/IP Client tried to write a non-writeable property in our gateway.
   j. “Invalid array index” –
      i. BACnet/IP Client tried to write a priority that was out of range or reserved (Priority 6) and was rejected.
      ii. BACnet/IP Client tried to write an array for an object or property that doesn’t have an array index.
   k. “Unknown device” – Gateway is trying to send a message to a device we have not had previous communication with on the network.
   l. “Timeout” – BACnet/IP message timed out.
   m. “Resources busy” – BACnet/IP message cannot be processed at this time.
   n. “Segmentation not supported” – BACnet/IP message is too large to send in one message.
   o. “Service not supported” – BACnet/IP Client tried to perform a service that our gateway does not support.
   p. “Abort Other” – BACnet/IP message is aborted for an unknown reason.
   q. “Invalid Tag” – BACnet/IP message is not how we expect.
   r. “Unknown” – BACnet/IP message error for an unknown reason.

LED Configuration

To modify the behavior of the LEDs on the 460 gateway, navigate to Other->Setup LEDs.

The LED Configuration page lets you configure the LEDs on the gateway.

Each LED may be set to Disabled, Protocol 1, or Protocol 2. If either Protocol is a Master/Client, you may set the LED to represent either all Slaves/Servers configured in our gateway or a particular Slave/Server device.

To select a particular Slave/Server device:

a) Select the protocol in the left dropdown menu.

b) Click **Save Parameters** to generate the second dropdown menu.

c) Select the individual Slave/Server in the right dropdown menu.

Click the **Save Parameters** button to commit the changes and reboot the gateway.

LED 1 is the LED closest to the Ethernet port on the gateway device.

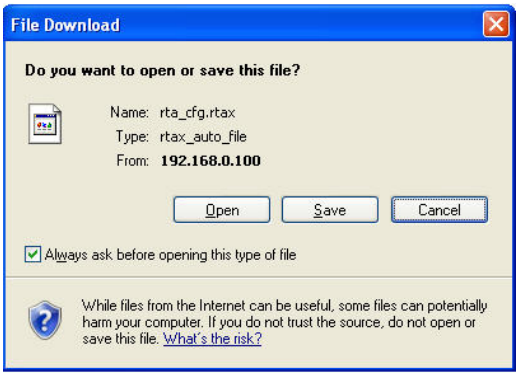
Configuration Files

To access the configuration files in the 460 gateway, navigate to other->Export/Import Config.

Export Configuration

The export tool allows you to save your gateway configuration for backup or to be exported into another gateway. This file is named *rta_cfg.rtax* by default. Network settings will not be saved in this configuration since they must be unique for each gateway.

Upon clicking the **Save Configuration to File** button, you will be prompted to select a location to save the file.


File Download
Do you want to open or save this file?
Name: rta_cfg.rtax
Type: rtax_auto_file
From: 192.168.0.100
Open
Save
Cancel
Always ask before opening this type of file
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

Import Configuration

You can import a previously exported configuration file or a configuration file from another device into the 460 gateway whenever it is in Configuration Mode.

Upon clicking the **Choose File** button, you will be prompted to select a location from which to load the saved file. Once the location is selected, click the **Load Configuration** button.

If it has successfully loaded, the gateway will indicate that it was successful and a message will appear under the Load Configuration button indicating you should reboot the gateway.

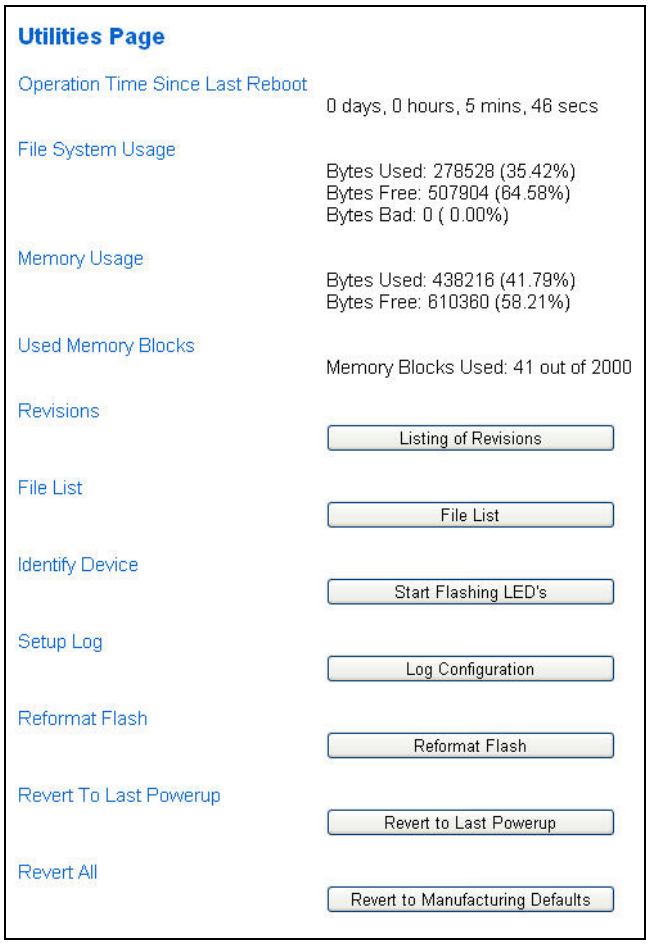
If it encountered an error while trying to load the saved configuration, the gateway will indicate the first error it found and a brief description about it under the Load Configuration button. The configuration file is xml and can be modified with any text editor. Once that error is fixed, try loading again until it is successful.

Utilities

The Utilities screen displays information about the gateway including Operation Time, File System Usage, Memory Usage, and Memory Block Usage.

Here you can also:

- View the Revisions of the Software for each Stack.
- View all of the Flash Files within the gateway.
- Identify your device by clicking the **Start Flashing LED's** button. By clicking this button, the two diagnostic LED's will flash red and green. Once you have identified which device you are working with, click the button again to put the LED's back into running mode.
- Configure the size of the Log through the Log Configuration.
- Remove the Configuration File and Flash Files within the gateway (the gateway needs to be rebooted 2 times).
- Bring the device back to its last power up settings.
- Bring the device back to its original manufacturing defaults (the Gateway needs to be rebooted 2 times).



Completing the Installation

You have now set up your gateway for communication and are ready to place the device in your application.

Support for your device is available any time.

Toll free: 800-249-1612
Email: support@rtaautomation.com